IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of	:	
Naoya TAKAO et al.	:	
Serial No. NEW	:	**Attn: APPLICATION BRANCH**
Filed July 22, 2003	:	Attorney Docket No. 2003_1017A

TERMINAL APPARATUS, COMMUNICATION METHOD, AND COMMUNICATION SYSTEM

THE COMMISSIONER IS AUTHORIZED TO CHARGE ANY DEFICIENCY IN THE FEES FOR THIS PAPER TO DEPOSIT ACCOUNT NO. 23-0975

CLAIM OF PRIORITY UNDER 35 USC 119

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicants in the above-entitled application hereby claim the date of priority under the International Convention of Japanese Patent Application No. 2002-213401, filed July 23, 2002, and Japanese Patent Application No. 2002-300108, filed October 15, 2002, as acknowledged in the Declaration of this application.

Certified copies of said Japanese Patent Applications are submitted herewith.

Respectfully submitted,

Naoya TAKAO et al.

By _____
Michael S. Huppert
Registration No. 40,268
Attorney for Applicants

MSH/kjf
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
July 22, 2003

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年　７月２３日

出願番号
Application Number: 特願２００２－２１３４０１

[ST.10/C]: [ＪＰ２００２－２１３４０１]

出願人
Applicant(s): 松下電器産業株式会社

２００３年　６月１２日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００３－３０４５９８７

【書類名】　特許願
【整理番号】　2032740081
【提出日】　平成14年 7月23日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 9/00
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　▲たか▼尾　直弥
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　杉山　圭司
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　森　俊也
【特許出願人】
【識別番号】　000005821
【氏名又は名称】　松下電器産業株式会社
【代理人】
【識別番号】　100097445
【弁理士】
【氏名又は名称】　岩橋　文雄
【選任した代理人】
【識別番号】　100103355
【弁理士】
【氏名又は名称】　坂口　智康

【選任した代理人】

【識別番号】　100109667

【弁理士】

【氏名又は名称】　内藤　浩樹

【手数料の表示】

【予納台帳番号】　011305

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9809938

【書類名】　明細書

【発明の名称】　グループ管理方法、グループ管理システム、グループ管理プログラム、およびグループ管理プログラムを記録した記録媒体

【特許請求の範囲】

【請求項１】　自分の公開鍵と秘密鍵を保持している加入依頼者が一人以上のメンバから構成されるグループにネットワークを介して新規加入するためのグループ加入方法であって、前記グループ固有の秘密鍵と公開鍵を保持する管理者に対して前記加入依頼者が少なくとも自分の公開鍵を送付して前記グループへの加入を依頼する加入依頼ステップと、前記管理者が少なくとも前記加入依頼者の公開鍵と前記グループ固有の秘密鍵に基づいて作成したグループ参加証を前記加入依頼者に送付する参加証発行ステップと、を実行することを特徴とするグループ加入方法。

【請求項２】　前記加入依頼ステップの前に前記管理者が偽者でないことを前記加入依頼者が確認する管理者確認ステップを実行することを特徴とする請求項１記載のグループ加入方法。

【請求項３】　前記加入依頼ステップにおいて前記加入依頼者が前記管理者に対して自分自身を特定する情報を追加して送付し、前記管理者が前記加入依頼者を特定する情報に基づき前記加入依頼者を加入させるか否かを判断する加入判断ステップを前記参加証発行ステップの前に実行することを特徴とする請求項１または請求項２に記載のグループ加入方法。

【請求項４】　第１から第３の請求項記載のグループ加入方法により前記グループ参加証を取得したメンバ間で前記グループへの加入資格を認証するためのグループ認証方法であって、認証者が被認証者に対して認証用文字列を送付する認証開始ステップと、前記被認証者が前記認証者に対して少なくとも前記認証用文字列から自分の秘密鍵に基づいて作成した応答文字列と前記グループ参加証を送付して認証を依頼する認証依頼ステップと、前記認証者が前記グループ参加証から前記グループ固有の公開鍵に基づいて前記被認証者の公開鍵を得て、次に前記応答文字列と前記被認証者の公開鍵から前記認証用文字列に一致する文字列が得られることを確認することをもって前記被認証者が前記グループの加入者である

ことを認証する認証ステップと、を実行することを特徴とするグループ認証方法。

【請求項５】　前記認証ステップの後に、前記認証者と前記被認証者が立場を入れ替えて前記グループ認証開始ステップから前記認証ステップまでを実行することを特徴とする請求項４記載のグループ認証方法。

【請求項６】　前記参加証発行ステップにおいて前記管理者が少なくとも前記加入依頼者の公開鍵、前記グループ参加証の有効期限に関する情報および前記グループ固有の秘密鍵に基づいて作成したグループ参加証を作成し前記加入依頼者に送付することを特徴とする請求項１から請求項３のいずれか１項に記載のグループ加入方法。

【請求項７】　前記認証ステップにおける前記被認証者の認証の際に、前記グループ参加証に含まれる有効期限に関する情報に基づいて前記被認証者が前記グループの有効な加入者であるかどうかも判断することを特徴とする請求項４または請求項５に記載のグループ認証方法。

【請求項８】　請求項６記載のグループ加入方法により前記グループ参加証を取得したメンバが前記グループ参加証の有効期限に関する情報を更新するためのグループ参加証更新方法であって、前記更新依頼者が前記管理者に対して少なくとも前記グループ参加証を送付して前記グループ参加証の有効期限に関する情報の更新を依頼する参加証更新依頼ステップと、前記管理者が前記グループ参加証から前記グループに固有の公開鍵に基づいて前記更新依頼者の公開鍵を得て、前記更新依頼者の公開鍵と新たな前記有効期限に関する情報および前記グループ固有の秘密鍵に基づいて作成した新たな前記グループ参加証を前記更新依頼者に送付する参加証更新ステップと、を実行することを特徴とするグループ参加証更新方法。

【請求項９】　前記参加証更新依頼ステップの前に前記管理者が偽者でないことを前記更新依頼者が確認する第２の管理者確認ステップを実行することを特徴とする請求項８記載のグループ参加証更新方法。

【請求項１０】　前記管理者が前記グループ参加証発行の権限を持つ発行者を追加する方法であって、発行者候補のメンバが少なくとも自分の公開鍵を前記管

理者へ送付する発行者鍵送付ステップと、前記管理者が少なくとも前記発行者候補の公開鍵と前記グループ固有の秘密鍵に基づいてグループ参加証発行許可証を作成し前記発行候補者に送付する参加証発行許可証発行ステップとを実行することを特徴とする発行者追加方法。

【請求項１１】　自分の公開鍵と秘密鍵を保持している加入依頼者が請求項１０記載の発行者追加方法により前記管理者からグループ参加証発行許可証の発行を受けた発行者からグループ参加証の発行を受ける第２のグループ加入方法であって、前記加入依頼者が少なくとも自分の公開鍵を送付して前記グループへの加入を依頼する第２の加入依頼ステップと、前記発行者が少なくとも前記加入依頼者の公開鍵と前記発行者の秘密鍵に基づいて作成したグループ参加証および前記発行者の前記グループ参加証発行許可証を前記加入依頼者に送付する第２の参加証発行ステップと、を実行することを特徴とする第２のグループ加入方法。

【請求項１２】　前記第２の加入依頼ステップの前に前記発行者が偽者でないことを前記加入依頼者が確認する発行者確認ステップを実行することを特徴とする請求項１１記載の第２のグループ加入方法。

【請求項１３】　前記第２の加入依頼ステップにおいて前記加入依頼者が前記発行者に対して自分自身を特定する情報を追加して送付し、前記発行者が前記加入依頼者を特定する情報に基づき前記加入依頼者を加入させるか否かを判断する第２の加入判断ステップを前記第２の参加証発行ステップの前に実行することを特徴とする請求項１１または請求項１２に記載の第２のグループ加入方法。

【請求項１４】　請求項１１から請求項１３のいずれか１項に記載の第２のグループ加入方法により前記グループ参加証を取得したメンバ間で前記グループへの加入資格を認証するための第２のグループ認証方法であって、認証者が被認証者に対して認証用文字列を送付する第２の認証開始ステップと、前記被認証者が前記認証者に対して少なくとも前記認証用文字列から自分の秘密鍵に基づいて作成した応答文字列と前記グループ参加証および前記グループ参加証発行許可証を送付して認証を依頼する第２の認証依頼ステップと、前記認証者が前記グループ参加証発行許可証から前記グループ固有の公開鍵に基づいて前記発行者の公開鍵を得て、次に前記グループ参加証から前記発行者の公開鍵に基づいて前記被認証

者の公開鍵を得て、さらに前記応答文字列と前記被認証者の公開鍵から前記認証用文字列に一致する文字列が得られることを確認することをもって前記被認証者が前記グループの加入者であることを認証する第２の認証ステップと、を実行することを特徴とする第２のグループ認証方法。

【請求項１５】　前記第２の認証ステップの後に、前記認証者と前記被認証者が立場を入れ替えて前記第２のグループ認証開始ステップから前記第２の認証ステップまでを実行することを特徴とする請求項１４記載の第２のグループ認証方法。

【請求項１６】　前記第２の参加証発行ステップにおいて、前記発行者が少なくとも前記加入依頼者の公開鍵、前記グループ参加証の有効期限に関する情報および前記発行者の秘密鍵に基づいて作成したグループ参加証を作成し前記加入依頼者に送付することを特徴とする請求項１１から請求項１３のいずれか１項に記載の第２のグループ加入方法。

【請求項１７】　前記第２の認証ステップにおいて前記グループ参加証に含まれる有効期限に関する情報に基づいて前記被認証者が前記グループの有効な加入者であるかどうかも判断することを特徴とする請求項１４または請求項１５に記載の第２のグループ認証方法。

【請求項１８】　請求項１６記載の第２のグループ加入方法により前記グループ参加証を取得したメンバが前記グループ参加証の有効期限に関する情報を更新するための第２のグループ参加証更新方法であって、前記更新依頼者が前記発行者に対して少なくとも前記グループ参加証を送付して前記グループ参加証の有効期限に関する情報の更新を依頼する第２の参加証更新依頼ステップと、前記発行者が前記グループ参加証発行許可証から前記グループに固有の公開鍵に基づいて前記グループ参加証発行許可証を発行した発行者の公開鍵を得て、次に前記グループ参加証から前記グループ参加証発行許可証を発行した発行者の公開鍵に基づいて前記更新依頼者の公開鍵を得て、さらに前記更新依頼者の公開鍵と新たな前記有効期限に関する情報および前記発行者の秘密鍵に基づいて作成した新たな前記グループ参加証を前記更新依頼者に送付する第２の参加証更新ステップと、を実行することを特徴とする第２のグループ参加証更新方法。

【請求項１９】　前記第２の更新依頼ステップの前に前記発行者が偽者でないことを前記更新依頼者が確認する発行者確認ステップを実行することを特徴とする請求項１８記載の第２のグループ参加証更新方法。

【請求項２０】　前記参加証発行許可証発行ステップにおいて、前記管理者が少なくとも前記発行者候補の公開鍵、前記グループ参加証発行許可証の有効期限に関する情報および前記グループ固有の秘密鍵に基づいてグループ参加証発行許可証を作成し前記発行候補者に送付することを特徴とする請求項１０記載の発行者追加方法。

【請求項２１】　前記第２の加入依頼ステップの前に前記グループ参加証発行許可証に含まれる有効期限に関する情報に基づいて前記発行者の前記グループ参加証発行許可証が有効かどうかも判断することを特徴とする請求項１１から請求項１３または請求項１６のいずれか１項に記載の第２のグループ加入方法。

【請求項２２】　前記第２の認証ステップにおいて前記グループ参加証発行許可証に含まれる有効期限に関する情報に基づいて前記被認証者が所有する前記グループ参加証発行許可証が有効かどうかも判断することを特徴とする請求項１４または請求項１５または請求項１７に記載の第２のグループ認証方法。

【請求項２３】　請求項１０記載の発行者追加方法により前記グループ参加証発行許可証の発行を受けた前記発行者が前記グループ参加証発行許可証の有効期限に関する情報を更新するための発行許可証更新方法であって、前記発行者が前記管理者に対して少なくとも前記グループ参加証発行許可証を送付して前記グループ参加証の有効期限に関する情報の更新を依頼する発行許可証更新依頼ステップと、前記管理者が前記グループ参加証発行許可証から前記グループに固有の公開鍵に基づいて前記発行者の公開鍵を得て、前記発行者の公開鍵と新たな前記有効期限に関する情報および前記発行者の秘密鍵に基づいて作成した新たな前記グループ参加証発行許可証を前記発行者に送付する発行許可証更新ステップと、を実行することを特徴とする発行許可証更新方法。

【請求項２４】　前記発行許可証更新依頼ステップの前に、前記管理者が偽者でないことを前記発行者が確認する第３の管理者確認ステップを実行することを特徴とする請求項２３記載の発行許可証更新方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ネットワークで接続された機器を使う複数のユーザがグループを構成し、情報をグループ内でのみ安全に共有するためのグループ管理方法に関する。

【０００２】

【従来の技術】

インターネットに接続してネットワークサービスを享受するユーザ数は、接続機器や接続料金の廉価化、接続機器の多彩化、および通信速度の向上などにより、急速に増加している。インターネット普及当初は、一部の情報提供者が提供する情報を一般ユーザがダウンロードする一方向のサービスが主流であったが、現在は自分の持つ情報、すなわちテキストデータ、静止画像データ、音声データ、動画像データなどを発信したいという一般ユーザも増え、主にＷＷＷ（Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ）などのサーバに自分の情報を複製し、他のユーザが閲覧可能とすることによってこれを実現している。

【０００３】

サーバで情報を公開するにあたっては、大きく分けて（１）サーバを自分で運用する、（２）サービス提供者が有料または無料で提供しているサーバに情報をアップロードする、という二つの方法がある。さらに、不特定多数を対象に発信するのではなく、友人・家族・共通の趣味を持つ者など特定ユーザ間（以下グループと呼ぶ）でのみプライベートな情報を共有したいという要求も増えているが、これを実現する方法としては、主に認証サーバを用いる方法すなわちグループへの参加を認められたユーザのユーザＩＤとパスワードの組（以下グループリスト）を認証サーバ（情報提供サーバと同一であっても良い）に登録しておき、ユーザが入力したユーザＩＤとパスワードの組を確認することによって当該グループでの情報共有を許可する方法などが用いられている。

【０００４】

このように情報提供者はサーバに情報を格納しておき、情報受信者がサーバへ

アクセスするというモデル（サーバークライアントモデルと呼ぶ）には、次の問題点がある。すなわち、自分でサーバで運用する場合には、（１）高度な知識が必要：サーバやネットワーク等に関する十分な知識が必要とされ、一般ユーザが運用することは困難な場合が多い、（２）コストがかかる：機材やソフトウェア以外にも、基本的に常時サービスを提供するためにサーバを常時稼動させるための運用費が必要となる、などの問題点があり、有料または無料で提供されるサーバを利用する場合には、（３）容量制限：多くの場合サーバに格納できる情報の容量には制限が設けられており、有料サーバの場合はコストをより多く負担することで容量制限を緩和することができるが、その場合にはより多くのコストがかかる、（４）プライバシ：サーバ提供者が信頼に足る場合であっても、何らかの事故等でサーバに格納した情報が第三者に漏れる場合があり、真にプライバシ保護を必要とする情報を共有することは困難である、などの問題点があり、共通の課題としては、（５）信頼性：サーバが何らかのトラブルでアクセス不能になった場合、情報発信や情報共有はまったく不可能となる、という問題点がある。なお、上で述べたコストに関する問題については、情報提供に対する収入によりコストを回収できるならば一定の負担は問題とならないが、一般ユーザが個人情報を発信あるいは共有する多くの場合はこれに当てはまらない。

【０００５】

上記のようなサーバークライアントモデルにおける情報共有時の問題点を解消するために近年着目されているのがピアートゥーピア（Ｐｅｅｒ－ｔｏ－Ｐｅｅｒ、以下Ｐ２Ｐ）モデルである。これは、情報をサーバに一極集中させず、必要なときに情報発信者－情報受信者間で直接伝送することで上記問題点を解決するものである。

【０００６】

Ｐ２Ｐモデルのネットワーク（以下Ｐ２Ｐネットワーク）に参加しているユーザ間で情報を転送する場合の流れを図１５にて例示する。各ユーザはＰ２Ｐネットワークに参加している他のユーザの存在を一人以上知っており、例えばＡはＢとＦ、ＢはＡとＣとＤ、ＥはＤのみの存在を知っている。この状態でＡが欲する情報を受信する際には、まず情報を持つユーザを特定するために検索を行う。

【０００７】

Ａはまず自分の知っているＢとＦに検索要求を発する。次にＢとＦはそれぞれが知っているユーザにこの検索要求を中継し、その先のユーザも同様に中継する（ステップ１５０１）。そしてこの検索要求に合致する情報を持っているユーザ、この場合はＣとＥは、Ａに対して情報を持っていることを直接通知し（ステップ１５０２）、Ａは何らかの判断基準でＥを選択してＡとＥの間で情報の転送が直接行われる（ステップ１５０３）。もちろん情報を分割してＣとＥの両者から同時に転送することも可能である。

【０００８】

これにより、前記サーバークライアントモデルの問題点（１）～（５）は次のように解決される。（１）サーバを運用しないため高度な知識は必要とされない。（２）またサーバを運用または利用するためのコストも不要である。（３）情報発信者Ｅから直接情報Ａを受信するので、転送可能な情報の容量はＡとＥのローカルな記録容量のみに制約され、実質的に容量の制限はない。（４）転送される情報はＡとＥ以外の第三者を経由しないので、既存技術でＡとＥの間の通信路を暗号化するなどすれば情報のプライバシは保たれる。（５）仮にＥがネットワークに参加していない状態（オフライン）であっても、ＡはＣから必要な情報を得ることができる。

【０００９】

さて、Ｐ２Ｐネットワークにおいてグループでの情報共有を行う場合には認証サーバが存在しないので、何らかの別の方法で各ユーザがそのグループに参加しているかどうかを互いに認証する必要がある。図１６を用いてその実現例と課題を説明する。

【００１０】

一つの方法はサーバークライアントモデルにおいて認証サーバが保持していたグループリストを当該グループに属する各ユーザが保持する方法である。図１６（１）において、ユーザＡ、Ｂ、Ｃはそれぞれグループリストを保持していて、グループリストにはグループを構成するユーザ（メンバ）としてＡとＢとＣが記述されている。各ユーザ、例えばＣが自分のユーザＩＤとパスワードを他のユー

ザ（ＡかつまたはＢ）に知らせると、ＡかつまたはＢはそのユーザＩＤとパスワードを自分が保持するグループリスト内の記述と比較する。比較結果が一致すればＣはグループのメンバであると認証され、ＡかつまたはＢとの間での情報共有を許可される。グループメンバではないユーザＸはグループリストに含まれるユーザＩＤとパスワードを知らないのでＡ、Ｂ、Ｃとの間での情報共有は許可されず、Ａ、Ｂ、Ｃからなるグループ内のプライバシが保たれる。

【００１１】

この第一の方法には次の問題がある。Ｃがオフライン時に、ＡまたはＢがＤを新たなメンバとしてグループに参加させたとする。その場合、図１６（２）に示すようにＡ、Ｂ、Ｄは、ＤのユーザＩＤとパスワードの記述が追加された新たなグループリストを共有することになる。この時点でＣはオフラインであるためこのグループリストの更新は通知されない。次にＡ、ＢがオフラインでＣ、Ｄのみがネットワーク参加状態（オンライン）になった場合（図１６（３））、Ｃは自分の保持するグループリストにはＤの記述がないためＤがグループメンバであることを認証できず、共にグループメンバであるＣ、Ｄの間でグループの情報共有が不可能になる。（Ｄの保持するグループリストにはＤ自身の記述があるが、Ｄがグループリストを改ざんして追加した可能性があるためＣはそれを信頼することはできない。）すなわち、この第一の方法では、グループリストを各ユーザがそれぞれ保持するが、その同期を保つことができないという問題点がある。

【００１２】

この問題を防ぐ第二の方法はグループリストを特定のメンバ一名のみが保持し、グループメンバの変更およびユーザのグループ参加状態の認証をこの特定メンバのみが行うことである。しかし、この第二の方法には、この特定メンバがオフラインの間は他のメンバ間で互いの認証ができなくなる問題がある。例えば図１６（４）においてＡがこの特定メンバであり、Ｂ、Ｃがグループメンバであるとする。Ａがオンラインであれば、ＢはＡに問い合わせることによりＣがグループメンバであることを認証できる。しかし、図１６（５）に示したようにＡがオフラインの場合、ＢはＡへの問い合わせが失敗するためＣを認証できず、共にグループメンバであるＢとＣの間で情報共有が不可能となる。

【００１３】

【発明が解決しようとする課題】

以上述べたように、サーバークライアントモデルの問題点を解決するためのＰ２Ｐネットワークにおいてグループでの情報共有を行う場合、（１）各ユーザがグループリストを保持する方法ではメンバ間のグループリストの同期が取れなくなる可能性がありその場合グループメンバ間であっても互いに認証することができないという問題点があり、また（２）特定メンバのみがグループリストを保持する方法ではその特定メンバがオフラインである間は他のメンバ間でグループメンバであることを互いに認証できなくなるという問題点がある。

【００１４】

本発明は、上記問題点に鑑み、グループでの情報共有にサーバの運用を必要とせず、かつ任意のメンバ間で常にグループメンバであることの認証が常に可能なグループ管理方法を提供することを目的とする。

【００１５】

【課題を解決するための手段】

本発明は、以上述べた課題を解決するため、以下のような構成をとるグループ加入方法、グループ認証方法、およびグループ参加証更新方法、ならびにこれらを含むグループ管理方法、グループ管理プログラム、およびこれを記録した記録媒体を提供する。または、発行者追加方法、第２のグループ加入方法、第２のグループ認証方法、第２のグループ参加証更新方法、および発行許可証更新方法、ならびにこれらを含むグループ管理方法、グループ管理プログラム、およびこれを記録した記録媒体を提供する。

【００１６】

グループ加入方法の一実施形態は、自分の公開鍵と秘密鍵を保持している加入依頼者が一人以上のメンバから構成されるグループにネットワークを介して新規加入するためのグループ加入方法であって、前記グループ固有の秘密鍵と公開鍵を保持する管理者に対して前記加入依頼者が少なくとも自分の公開鍵を送付して前記グループへの加入を依頼する加入依頼ステップと、前記管理者が少なくとも前記加入依頼者の公開鍵と前記グループ固有の秘密鍵に基づいて作成したグルー

プ参加証を前記加入依頼者に送付する参加証発行ステップと、を実行することを特徴とする。

【００１７】

また、グループ加入方法の一実施形態においては、前記加入依頼ステップの前に前記管理者が偽者でないことを前記加入依頼者が確認する管理者確認ステップを実行することを特徴とする。

【００１８】

また、グループ加入方法の一実施形態においては、前記加入依頼ステップにおいて前記加入依頼者が前記管理者に対して自分自身を特定する情報を追加して送付し、前記管理者が前記加入依頼者を特定する情報に基づき前記加入依頼者を加入させるか否かを判断する加入判断ステップを前記参加証発行ステップの前に実行することを特徴とする。

【００１９】

また、グループ加入方法の一実施形態においては、前記参加証発行ステップにおいて前記管理者が少なくとも前記加入依頼者の公開鍵、前記グループ参加証の有効期限に関する情報および前記グループ固有の秘密鍵に基づいて作成したグループ参加証を作成し前記加入依頼者に送付することを特徴とする。

【００２０】

グループ認証方法の一実施形態は、グループ加入方法により前記グループ参加証を取得したメンバ間で前記グループへの加入資格を認証するためのグループ認証方法であって、認証者が被認証者に対して認証用文字列を送付する認証開始ステップと、前記被認証者が前記認証者に対して少なくとも前記認証用文字列から自分の秘密鍵に基づいて作成した応答文字列と前記グループ参加証を送付して認証を依頼する認証依頼ステップと、前記認証者が前記グループ参加証から前記グループ固有の公開鍵に基づいて前記被認証者の公開鍵を得て、次に前記応答文字列と前記被認証者の公開鍵から前記認証用文字列に一致する文字列が得られることを確認することをもって前記被認証者が前記グループの加入者であることを認証する認証ステップと、を実行することを特徴とする。

【００２１】

また、グループ認証方法の一実施形態においては、前記認証ステップの後に、前記認証者と前記被認証者が立場を入れ替えて前記グループ認証開始ステップから前記認証ステップまでを実行することを特徴とする。

【００２２】

また、グループ認証方法の一実施形態においては、前記認証ステップにおける前記被認証者の認証の際に、前記グループ参加証に含まれる有効期限に関する情報に基づいて前記被認証者が前記グループの有効な加入者であるかどうかも判断することを特徴とする。

【００２３】

グループ参加証更新方法の一実施形態は、グループ加入方法により前記グループ参加証を取得したメンバが前記グループ参加証の有効期限に関する情報を更新するためのグループ参加証更新方法であって、前記更新依頼者が前記管理者に対して少なくとも前記グループ参加証を送付して前記グループ参加証の有効期限に関する情報の更新を依頼する参加証更新依頼ステップと、前記管理者が前記グループ参加証から前記グループに固有の公開鍵に基づいて前記更新依頼者の公開鍵を得て、前記更新依頼者の公開鍵と新たな前記有効期限に関する情報および前記グループ固有の秘密鍵に基づいて作成した新たな前記グループ参加証を前記更新依頼者に送付する参加証更新ステップと、を実行することを特徴とする。

【００２４】

また、グループ参加証更新方法の一実施形態においては、前記参加証更新依頼ステップの前に前記管理者が偽者でないことを前記更新依頼者が確認する第２の管理者確認ステップを実行することを特徴とする。

【００２５】

発行者追加方法の一実施形態は、前記管理者が前記グループ参加証発行の権限を持つ発行者を追加する方法であって、発行者候補のメンバが少なくとも自分の公開鍵を前記管理者へ送付する発行者鍵送付ステップと、前記管理者が前記発行者候補の公開鍵と前記グループ固有の秘密鍵に基づいてグループ参加証発行許可証を作成し前記発行候補者に送付する参加証発行許可証発行ステップとを実行することを特徴とする。

【００２６】

また、発行者追加方法の一実施形態は、前記参加証発行許可証発行ステップにおいて、前記管理者が少なくとも前記発行者候補の公開鍵、前記グループ参加証発行許可証の有効期限に関する情報および前記グループ固有の秘密鍵に基づいてグループ参加証発行許可証を作成し前記発行候補者に送付することを特徴とする。

【００２７】

第２のグループ加入方法の一実施形態は、自分の公開鍵と秘密鍵を保持している加入依頼者が、前述の発行者追加方法により前記管理者からグループ参加証発行許可証の発行を受けた発行者からグループ参加証の発行を受ける第２のグループ加入方法であって、前記加入依頼者が少なくとも自分の公開鍵を送付して前記グループへの加入を依頼する第２の加入依頼ステップと、前記発行者が少なくとも前記加入依頼者の公開鍵と前記発行者の秘密鍵に基づいて作成したグループ参加証および前記発行者の前記グループ参加証発行許可証を前記加入依頼者に送付する第２の参加証発行ステップと、を実行することを特徴とする。

【００２８】

また、第２のグループ加入方法の一実施形態は、前記第２の加入依頼ステップの前に前記発行者が偽者でないことを前記加入依頼者が確認する発行者確認ステップを実行することを特徴とする。

【００２９】

また、第２のグループ加入方法の一実施形態は、前記第２の加入依頼ステップにおいて前記加入依頼者が前記発行者に対して自分自身を特定する情報を追加して送付し、前記発行者が前記加入依頼者を特定する情報に基づき前記加入依頼者を加入させるか否かを判断する第２の加入判断ステップを前記第２の参加証発行ステップの前に実行することを特徴とする。

【００３０】

また、第２のグループ加入方法の一実施形態は、前記第２の参加証発行ステップにおいて、前記発行者が少なくとも前記加入依頼者の公開鍵、前記グループ参加証の有効期限に関する情報および前記発行者の秘密鍵に基づいて作成したグル

ープ参加証を作成し前記加入依頼者に送付することを特徴とする。

【００３１】

また、第２のグループ加入方法の一実施形態は、前記第２の加入依頼ステップの前に前記グループ参加証発行許可証に含まれる有効期限に関する情報に基づいて前記発行者の前記グループ参加証発行許可証が有効かどうかも判断することを特徴とする。

【００３２】

第２のグループ認証方法の一実施形態は、第２のグループ加入方法により前記グループ参加証を取得したメンバ間で前記グループへの加入資格を認証するための第２のグループ認証方法であって、認証者が被認証者に対して認証用文字列を送付する第２の認証開始ステップと、前記被認証者が前記認証者に対して少なくとも前記認証用文字列から自分の秘密鍵に基づいて作成した応答文字列と前記グループ参加証および前記グループ参加証発行許可証を送付して認証を依頼する第２の認証依頼ステップと、前記認証者が前記グループ参加証発行許可証から前記グループ固有の公開鍵に基づいて前記発行者の公開鍵を得て、次に前記グループ参加証から前記発行者の公開鍵に基づいて前記被認証者の公開鍵を得て、さらに前記応答文字列と前記被認証者の公開鍵から前記認証用文字列に一致する文字列が得られることを確認することをもって前記被認証者が前記グループの加入者であることを認証する第２の認証ステップと、を実行することを特徴とする。

【００３３】

また、第２のグループ認証方法の一実施形態は、前記第２の認証ステップの後に、前記認証者と前記被認証者が立場を入れ替えて前記第２のグループ認証開始ステップから前記第２の認証ステップまでを実行することを特徴とする。

【００３４】

また、第２のグループ認証方法の一実施形態は、前記第２の認証ステップにおいて前記グループ参加証に含まれる有効期限に関する情報に基づいて前記被認証者が前記グループの有効な加入者であるかどうかも判断することを特徴とする。

【００３５】

また、第２のグループ認証方法の一実施形態は、前記第２の認証ステップにお

いて前記グループ参加証発行許可証に含まれる有効期限に関する情報に基づいて前記被認証者が所有する前記グループ参加証発行許可証が有効かどうかも判断することを特徴とする。

【００３６】

第２のグループ参加証更新方法の一実施形態は、第２のグループ加入方法により前記グループ参加証を取得したメンバが前記グループ参加証の有効期限に関する情報を更新するための第２のグループ参加証更新方法であって、前記更新依頼者が前記発行者に対して少なくとも前記グループ参加証を送付して前記グループ参加証の有効期限に関する情報の更新を依頼する第２の参加証更新依頼ステップと、前記発行者が前記グループ参加証発行許可証から前記グループに固有の公開鍵に基づいて前記グループ参加証発行許可証を発行した発行者の公開鍵を得て、次に前記グループ参加証から前記グループ参加証発行許可証を発行した発行者の公開鍵に基づいて前記更新依頼者の公開鍵を得て、さらに前記更新依頼者の公開鍵と新たな前記有効期限に関する情報および前記発行者の秘密鍵に基づいて作成した新たな前記グループ参加証を前記更新依頼者に送付する第２の参加証更新ステップと、を実行することを特徴とする。

【００３７】

また、第２のグループ参加証更新方法の一実施形態は、前記第２の参加証更新依頼ステップの前に前記発行者が偽者でないことを前記更新依頼者が確認する発行者確認ステップを実行することを特徴とする。

【００３８】

発行許可証更新方法の一実施形態は、発行者追加方法により前記グループ参加証発行許可証の発行を受けた前記発行者が前記グループ参加証発行許可証の有効期限に関する情報を更新するための発行許可証更新方法であって、前記発行者が前記管理者に対して少なくとも前記グループ参加証発行許可証を送付して前記グループ参加証の有効期限に関する情報の更新を依頼する発行許可証更新依頼ステップと、前記管理者が前記グループ参加証発行許可証から前記グループに固有の公開鍵に基づいて前記発行者の公開鍵を得て、前記発行者の公開鍵と新たな前記有効期限に関する情報および前記発行者の秘密鍵に基づいて作成した新たな前記

グループ参加証発行許可証を前記発行者に送付する発行許可証更新ステップと、を実行することを特徴とする。

【００３９】

また、発行許可証更新方法の一実施形態は、前記発行許可証更新依頼ステップの前に、前記管理者が偽者でないことを前記発行者が確認する第３の管理者確認ステップを実行することを特徴とする。

【００４０】

第１のグループ管理プログラムの一実施形態は、前記グループ加入方法における前記加入依頼ステップまたは前記管理者確認ステップおよび前記加入依頼ステップ、および前記グループ認証方法における前記認証依頼ステップおよび前記認証開始ステップおよび前記認証ステップ、を実行することが記述されていることを特徴とする。

【００４１】

また、第１のグループ管理プログラムの一実施形態は、前記グループ参加証更新方法における前記参加証更新依頼ステップ、または前記第２の管理者確認ステップおよび前記参加証更新依頼ステップを実行することが記述されていることを特徴とする。

【００４２】

第２のグループ管理プログラムの一実施形態は、前記グループ加入方法における前記参加証発行ステップまたは前記加入判断ステップおよび前記参加証発行ステップを実行することが記述されていることを特徴とする。

【００４３】

また、第２のグループ管理プログラムの一実施形態は、前記グループ参加証更新方法における前記参加証更新ステップを実行することが記述されていることを特徴とする。

【００４４】

第３のグループ管理プログラムの一実施形態は、前記第２のグループ加入方法における前記第２の加入依頼ステップまたは前記発行者確認ステップおよび前記第２の加入依頼ステップ、および前記第２のグループ認証方法における前記第２

の認証依頼ステップおよび前記第２の認証開始ステップおよび前記第２の認証ステップを実行することが記述されていることを特徴とする。

【００４５】

また、第３のグループ管理プログラムの一実施形態は、前記第２のグループ参加証更新方法における第２の参加証更新依頼ステップを実行することが記述されていることを特徴とする。

【００４６】

また、第３のグループ管理プログラムの一実施形態は、前記第２のグループ参加証更新方法における前記発行者確認ステップを実行することを特徴とする。

【００４７】

第４のグループ管理プログラムの一実施形態は、前記発行者追加方法における前記発行者鍵送付ステップ、および前記第２のグループ加入方法における前記第２の参加証発行ステップ、およびを実行することが記述されていることを特徴とする。

【００４８】

また、第４のグループ管理プログラムの一実施形態は、前記発行許可証更新方法における前記発行許可証更新依頼ステップを実行することが記述されていることを特徴とする。

【００４９】

また、第４のグループ管理プログラムの一実施形態は、前記発行許可証更新方法における前記第３の管理者確認ステップを実行することが記述されていることを特徴とする。

【００５０】

第５のグループ管理プログラムの一実施形態は、前記発行者追加方法における前記参加証発行許可証発行ステップ、および前記発行許可証更新方法における前記発行許可証更新ステップを実行することが記述されていることを特徴とする。

【００５１】

グループ管理プログラムを記録する記録媒体の一実施形態は、前記第１から第５のグループ管理プログラムの一部または全部が記録されていることを特徴とす

る。

【００５２】

第１のグループ管理システムの一実施形態は、少なくとも前記第１のグループ管理プログラムを実行可能な状態で保持する第１の端末と、少なくとも前記第２のグループ管理プログラムを実行可能な状態で保持する第２の端末と、から少なくとも構成されることを特徴とする。

【００５３】

第２のグループ管理システムの一実施形態は、少なくとも前記第３のグループ管理プログラムを実行可能な状態で保持する第３の端末と、少なくとも前記第４のグループ管理プログラムを実行可能な状態で保持する第４の端末と、少なくとも前記第５のグループ管理プログラムを実行可能な状態で保持する第５の端末と、から少なくとも構成されることを特徴とする。

【００５４】

本願発明は、以下の記載の「発明の実施の形態」および添付の図面を用いて説明されるが、これは例示を目的とするものであって、本願発明は、これらに限定されるものではない。

【００５５】

【発明の実施の形態】

まず、本発明の実施形態の構成について概要を説明する。本発明はネットワークで互いに接続された複数の機器間の通信方法に関するものである。

【００５６】

本発明はイーサネット、アナログまたはデジタルの公衆回線または専用回線を用いたネットワーク、ＡＤＳＬ（Ａｓｙｍｍｅｔｒｉｃ　Ｄｉｇｉｔａｌ　Ｓｕｂｓｃｒｉｂｅｒ　Ｌｉｎｅ）、無線ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）などの物理的なネットワークを想定しているが、これらに制限されるものではない。また、インターネットではネットワークの下位プロトコルとしてＴＣＰ／ＩＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｒｏｌ　Ｐｒｏｔｏｃｏｌ／Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）が広く使用されており本発明もその使用を想定しているが、これに制限されるものでもない。

【００５７】

前記機器のそれぞれに前記物理的なネットワークに対応した通信インタフェースが備わっており、前記通信インタフェースを制御して通信を行うためのプログラムを前記機器内のＣＰＵが実行することにより通信処理が行われる。前記プログラムは前記機器のＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）に記録されている場合、あるいは前記機器のハードディスクやリムーバブルディスクなど不揮発記憶装置に格納されていてそこから必要に応じて前記機器のＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）に読み込まれて実行される場合、あるいはこれらを組み合わせて実行する場合などがある。

【００５８】

また前記機器には機器使用者の入力を受け付けるための入力手段も備わっている。入力手段としては通常キーボード、マウス、タブレットなどが用いられる。これらの構成についてはパーソナルコンピュータなどで一般的に知られているものであり、本発明の主眼ではないので詳細な説明は省略する。

【００５９】

なお、以下で用いる「ユーザ」という用語は、前記機器、前記機器で動作するプログラムおよび機器使用者を含む概念である。本発明が想定しているネットワークにおいては、各ユーザは、必ずしも常時ネットワークに接続しているわけではなく、通信に必要な各ユーザのアドレス情報（ＩＰアドレス、ポート番号など）も固定ではなくネットワークに接続するたびに変化する可能性がある。

【００６０】

（実施の形態１）

本発明の第一の実施の形態について説明する。

【００６１】

まず、本実施の形態で用いている公開鍵暗号化方式の概要を説明する。公開鍵暗号化方式とは、次のような数学的性質を持つ二つの暗号鍵、「公開鍵」と「秘密鍵」を用いた暗号化方式である。（１）公開鍵と秘密鍵は、一方から現実的な時間で他方を計算することが互いに不可能である。（２）公開鍵で暗号化した情報は対応する秘密鍵でのみ復号可能であり、逆もまた成立する。

【００６２】

上記（１）の性質により、利用者は秘密鍵のみを秘密裡に保持しておけば、公開鍵を第三者に知られても問題ないので公開鍵を公開しておくことができる。従って、情報を秘密裡に送信したい送信者は、前もって受信者の公開鍵を入手しておき情報を受信者の公開鍵で暗号化したものを送信する。受信者は自分のみが持つ秘密鍵でそれを復号することができ、暗号化前の情報を得ることができる。第三者が暗号化された情報を傍受しても、受信者の秘密鍵でしか復号できないため情報が漏洩することはない。以下では、暗号化対象の情報Ｍを鍵Ｋで暗号化したものをｅ（Ｍ，Ｋ）のように表記することとする。

【００６３】

また、公開鍵暗号化方式を用いて、情報そのものは暗号化しないが、情報が改ざんされていないことを証明するための電子「署名」を行うことも可能である。すなわち、署名対象の情報Ｍから所定のアルゴリズムｆで一意に導き出される派生情報Ｈ＝ｆ（Ｍ）を送信者の秘密鍵ＫＳで暗号化したＳｇｎ＝ｅ（Ｈ，ＫＳ）を署名情報として元の情報Ｍに付加して送信する。受信者は、ＭとＳｇｎを受信し、Ｓｇｎを送信者の公開鍵ＫＰで復号化してＨを得て、Ｈ＝ｆ（Ｍ）が成立することを確認することで情報Ｍが第三者によって改ざんされていないことを確認できる。なぜならばＭが第三者により改ざんされていればＨ＝ｆ（Ｍ）が成立せず、また送信者の秘密鍵ＫＳがなければ、送信者の公開鍵ＫＰで正常に復号できるＳｇｎの作成も不可能だからである。

【００６４】

公開鍵暗号化方式およびこれを応用した署名方式は、インターネットでセキュリティを要する通信に広く用いられている。以下では、あるユーザＡの公開鍵、秘密鍵をそれぞれＫＡ＿Ｐ、ＫＡ＿Ｓのように表記する。

【００６５】

本願においてグループは次のように定義する。（１）グループは一名以上のネットワーク参加者からなる（２）一ユーザは複数のグループに属することが可能である（３）グループにはグループ固有の共有情報がある（４）同じグループに属することを互いに認証されたメンバ間ではそのグループの共有情報の送受信を

行うことができる。グループを構成するメンバは、友人、家族、同じ趣味の持ち主、住所が近い者、の集合などが考えられる。

【００６６】

本実施の形態においては、グループを構成するメンバをグループ参加証を発行する権限をもつ管理者および一般ユーザに分類する。一般ユーザにグループ参加証を発行できるのは管理者のみであり、ユーザはグループ参加証を管理者に発行してもらうことでグループへの参加が可能となる。本願において、グループ参加証とは、あるグループのメンバが、他のグループメンバに対して、当該グループに参加していることを証明するための情報であると定義される。

【００６７】

このようなグループを管理するには、以下に示すような処理が必要となる。

【００６８】

（１）グループの生成

（２）グループの告知

（３）グループの発見

（４）グループ管理者の特定

（５）グループへの新規加入依頼

（６）グループメンバ間の認証

（７）グループメンバ間の情報共有

（８）グループ参加証の更新

（９）グループメンバの削除

（１０）グループ管理者の追加

（１１）グループ公開鍵の更新

以下、各処理について説明する。

【００６９】

１．グループの生成

情報共有のためにグループを作成したいユーザＡは、そのグループ用の公開鍵ＫＧ＿Ｐおよび秘密鍵ＫＧ＿Ｓのペアを作成する。これらはＡが指定した情報（パスフレーズ）を元に生成されたものであってもよいし、プログラムまたは装置

が生成した乱数などの情報を元に生成されたものであってもよい。

【００７０】

２．グループの告知

生成したグループ公開鍵ＫＧ＿Ｐは、そのグループを特定する情報、例えば望ましくは他のグループと重複しないグループＩＤと共に何らかの方法でグループ情報として告知される。この告知方法としては、（１）従来の技術の説明に用いた図１５にて例示したようなＰ２Ｐネットワークの全てあるいは一部のユーザを宛て先としてＡがグループ情報を発信し、そのグループ情報が図１５の検索情報の流れのようにユーザからユーザへと順次転送され、最終的に宛て先とされたユーザが受信することで実現してもよいし、（２）物理的にＡと同じローカルエリアネットワーク（ＬＡＮ）または仮想プライベートネットワーク（ＶＰＮ）に属している他のユーザ宛てにグループ情報をブロードキャストすることで実現してもよいし、あるいは、（３）Ａが電子メール、郵便等を含む、Ｐ２Ｐネットワークを介した転送以外の何らかの方法で他のユーザに対して少なくともグループ公開鍵ＫＧ＿Ｐを直接送信することで実現してもよいし、さらには、（４）グループ情報のリストを保持し検索の用途に供するグループ情報インデックスサーバを運営し、前記グループ情報をこのグループ情報インデックスサーバに登録することによって実現してもよいし、（５）これらを複数組み合わせて実現することも可能である。

【００７１】

なお、前記グループ情報には、そのグループ名、グループの生成者を特定する情報、成り立ち、目的、参加条件等、当該グループの内容を説明する情報と共に告知されていても構わないし、グループ公開鍵ＫＧ＿Ｐのみをグループ情報として告知しても構わない。

【００７２】

３．グループの発見

Ｐ２Ｐネットワークに参加しているユーザＸは、次のいずれかの方法でグループを発見し、グループを特定する情報、少なくともグループ公開鍵ＫＧ＿Ｐを入手する。（１）Ｘが保持している、過去に告知され受信したグループ情報（グル

ープを生成したＡから直接受け取ったグループ情報を含む）から、グループを特定する情報あるいはグループを説明する情報に基づき所望のグループを発見する。（２）図１５に例示したようなＰ２Ｐネットワークの情報検索の仕組みを用いて他のユーザに対してグループを特定する情報あるいはグループを説明する情報の一部または全部をキーとして検索し、該当するグループ情報を保持しているユーザからグループ情報を入手する。（３）前記グループ情報インデックスサーバが運用されている場合には、このグループ情報インデックスサーバに対してグループを特定する情報あるいはグループを説明する情報の一部または全部をキーとして検索し、所望のグループのグループ情報を入手する。（４）グループを生成したＡがＸにとって既知の場合は、グループ情報をＡから何らかの手段で直接入手する。

【００７３】

４．グループ管理者の特定

グループ管理者とは、グループメンバの追加削除の権限を持つユーザであり、より具体的にはグループ秘密鍵ＫＧ＿Ｓを保持するユーザである。あるグループへ新規加入したいユーザＸは、５．で説明するようにグループ管理者Ａと直接通信する必要があり、そのために必要なグループ管理者Ａのアドレス情報、例えばＩＰアドレス、通信に用いるポート番号、などを特定する必要がある。それは例えば次のいずれかの方法で行われる。（１）Ｘは図１５に例示したようなＰ２Ｐネットワークの情報検索の仕組みを用いてグループを特定する情報の一部または全部をキーとして検索を行い、この検索要求を受けた該当するグループの管理者がこれに応答し、自分のアドレス情報をＸに対して通知する。（２）ピア情報サーバを用いる方法である。ピア情報サーバとは、現在オンライン状態である全ユーザ、あるいは少なくとも一つのグループの管理者である全ユーザの、少なくともアドレス情報および当該ユーザが管理者であるグループのグループを特定する情報を収集して検索の用途に供するサーバである。Ｘはこのピア情報サーバに対してグループを特定する情報をキーとして検索を行い、その検索結果として管理者のアドレス情報を入手する。（３）グループ管理者ＡがＸにとって既知であり、かつグループ管理者Ａが常にオンラインであってアドレス情報が変化しないこ

とも既知である場合、そのアドレス情報を用いる。

【００７４】

５．グループへの新規加入依頼

あるグループへ新規加入したいユーザＸは、前記４．で特定したアドレス情報を用いてグループ管理者Ａと通信を行い、６．で必要となるグループ参加証の発行を依頼する。本処理の詳細については後述する。

【００７５】

６．グループメンバ間の認証

前記５．で入手したグループ参加証を持つグループメンバ間では、互いに同じグループに属していることを認証することが可能になる。本処理の詳細については後述する。

【００７６】

７．グループメンバ間の情報共有

前記６．で互いに同じグループに属していると認証された複数のグループメンバ間、例えばＸとＹの間ではグループの共有情報の相互の転送が可能になる。これは、例えば次のようなステップを順に実行することにより行われる。

【００７７】

（７－１）通信に用いる暗号鍵の設定

前記６．で互いに同じグループに属していることを認証した後、暗号鍵Ｋ＿ＸＹを一方、例えばＸ、が作成して、Ｘの秘密鍵およびＹの公開鍵でこの暗号鍵を暗号化してＹに送付する。Ｙはこれを自分の秘密鍵およびＸの公開鍵を用いて復号可能であり、またＹ以外はこれを復号することができない。これにより、安全にＫ＿ＸＹをＸからＹに通知する。

【００７８】

（７－２）情報転送の暗号化

以降のＸとＹの間の情報転送は、共通鍵Ｋ＿ＹＸで暗号化して行う。第三者はＫ＿ＸＹを知ることができないので、ＸＹ間の通信を傍受してもその内容を復号することはできず、またＸまたはＹに成りすまして偽の情報をＹまたはＸに転送することも不可能となり、ＸとＹは安全に情報転送を行うことができる。これに

より、グループメンバ相互間での安全なグループ情報の共有が可能となる。

【００７９】

なお、３名以上のメンバがお互いに認証された状態である場合、このメンバ間の情報転送に用いる暗号鍵には次のような選択肢がある。

【００８０】

（１）異なる二者間の通信には異なる暗号鍵を用いる。例えば、ＡとＢとＣが互いに認証されている場合、ＡとＢの間の通信には暗号鍵Ｋ＿ＡＢを、ＢＣ間はＫ＿ＢＣ、ＣＡ間はＫ＿ＣＡを用いる方法である。

【００８１】

（２）互いに認証された複数メンバ間で共通の暗号鍵を用いる。例えば、ＡとＢが互いに認証されていて暗号鍵Ｋ＿ＡＢを用いて通信している状態でＣが新たにＡまたはＢとの認証処理を行って認証された場合、ＡまたはＢからＣへＣの公開鍵を用いて安全にＫ＿ＡＢを送付し、以降はＡ、Ｂ、Ｃのいずれの二者間でも暗号鍵Ｋ＿ＡＢを用いる方法である。

【００８２】

８．グループ参加証の更新

前記５．で発行されるグループ参加証に有効期限情報が含まれている場合には、当該有効期限以降、グループへの参加（グループメンバ間の認証）が不可能になるため、ユーザはグループ参加証の更新が必要となる。本処理の詳細については後述する。

【００８３】

９．グループメンバの削除

上記で述べてきた方法では、グループ参加証を持つユーザは、そのグループ参加証の有効期限まではグループへの参加が可能であるが、何らかの理由により、その有効期限以前にそのユーザをグループメンバから除外したい（そのユーザをグループメンバとして認証できないようにしたい）場合は、例えば次のような処理を実行することで可能となる。グループメンバの削除について、グループ参加証の消去（下記（９－１））および失効者情報の作成（下記（９－２－１）～（９－２－４））の２例を挙げて説明する。

【００８４】

（９－１）グループ参加証の消去

除外対象メンバが保持しているグループ参加証を消去すれば、当該メンバはその後は前記６．で述べたグループメンバ間の認証が行えなくなる。そのためには次のような処理を実行する必要がある。

【００８５】

（９－１－１）グループ参加証の消去指示

グループ管理者がメンバを除外することを指定することを指示する参加証消去指示ステップを実行する。

【００８６】

（９－１－２）グループ参加証の消去

上記参加証消去指示を受けた当該メンバは、自分が保持しているグループ参加証を消去する。これは機器の使用者が手動で消去する方法でも良いが、この場合は指示を無視して故意に消去しない場合も考えられるので、上記参加証消去指示を受けた機器あるいはプログラムが強制的に消去する方法でもよい。

【００８７】

（９－２－１）失効者情報の作成

グループメンバの一人（グループ管理者含む）が、除外されたメンバを特定する情報、例えば当該メンバの公開鍵、を含む失効者情報を作成する。

【００８８】

（９－２－２）失効者リストの共有前記６．のグループメンバ間の認証の際には、自分が保持する失効者情報のリストと認証相手が持つ失効者情報のリストを比較し、一方が保持しない失効者情報が存在する場合は互いに他方の失効者リストに追加することで、失効者情報のリストを全グループメンバで共有するようにする。

【００８９】

（９－２－３）失効者の除外

前記６．のグループメンバ間の認証の際に、認証相手が自分の保持する失効者リストに含まれているかどうかを確認し、含まれている場合は相手をグループメ

ンバであると認証しない。例えばユーザの公開鍵を失効者情報として用いる場合は、認証相手の公開鍵がリストに含まれる失効者情報のいずれかと一致すれば、この相手の認証を拒否する。

【００９０】

（９－２－４）失効者の参加資格更新の拒否

前記８．においてグループ参加証の更新を行う際に、参加証の更新を依頼したユーザがリストに含まれる失効者情報のいずれかと一致するかどうかを確認し、一致するものがある場合は参加証の更新を拒否する。

【００９１】

なお、失効者情報にその消去期限を含めておいて、消去期限を越えた失効者情報を削除することが可能である。例えば、グループ参加証の有効期限より少し後の時点を消去期限として付与しておけば、不要となった失効者情報を順次削除することができ、失効者情報のリストが無限に増大することを防ぐことができる。

【００９２】

また、失効者情報の作成はグループ管理者のみが行い、グループ管理者がグループ秘密鍵ＫＧ＿Ｓを用いて暗号化した状態で共有することとしてもよい。グループメンバは公開されているグループ公開鍵ＫＧ＿Ｐを用いて失効者情報を復号することが可能であり、この失効者情報が不正に改ざんされていないことの確認が可能となる。これにより、悪意を持つユーザにより作成された不正な失効者情報が共有されることを防ぐことができる。

【００９３】

また、グループ参加証の消去（上記（９－１））の方法と、失効者情報の作成（上記（９－２－１）～（９－２－４））による方法とを、必要に応じて組み合わせることによって、目的のメンバを削除してもよい。

【００９４】

１０．グループ管理者の追加

前記５．で述べたグループへの新規加入は、グループ管理者がオンラインである場合にしか行えない。グループ生成直後はグループを生成したユーザ一人のみがグループ管理者であるが、グループへの新規加入の機会を増やすために、グル

ープ管理者を増やすことが可能である。これは、グループ秘密鍵ＫＧ＿Ｓを何らかの安全な手段、すなわち暗号化通信または郵送などの手段によってグループ管理者から別のユーザ（追加されるべき別のグループ管理者）に転送することによって実現することができる。

【００９５】

１１．グループ公開鍵の更新

何らかの事故によりグループ秘密鍵ＫＧ＿Ｓがグループ管理者以外のユーザに漏洩した場合、グループ秘密鍵を入手したユーザは不正にグループ参加証または失効者リストを発行することが可能となり、かつグループメンバには本来のグループ管理者が発行したグループ参加証と不正に発行されたグループ参加証を判別することはできない。このような場合には、グループ公開鍵・秘密鍵のペアを更新する以外に不正を防ぐ方法はない。また、前記１０．で追加されたグループ管理者のいずれかからユーザ追加削除の権限を剥奪したい場合も、グループ公開鍵・秘密鍵のペアを更新する以外の方法はない。一方、グループ管理者がグループ公開鍵・秘密鍵をそれぞれＫＧ＿Ｐ’、ＫＧ＿Ｓ’に更新したとしても、従来のグループ公開鍵ＫＧ＿Ｐとそれに基づいて作成されたグループ参加証を持つグループメンバ同士では前記６．のグループ認証は互いに可能なままなので、グループメンバは常に最新のグループ公開鍵を保持しておく必要があると同時に、最新のグループ公開鍵に対応したグループ参加証を入手する必要がある。

【００９６】

最新のグループ公開鍵の保持は、例えば次のいずれかのような方法により可能である。

【００９７】

（１）グループ管理者がグループ公開鍵・秘密鍵を更新した時点で、図１５に例示したようなＰ２Ｐネットワークを介してネットワーク参加者全員に新しいグループ公開鍵を送付する。対応するグループのメンバは、この新しいグループ公開鍵で自分が保持しているグループ公開鍵を置き換える。

【００９８】

（２）前記２．で告知されるグループ情報に、グループ公開鍵の更新時刻に関

する情報も含めておき、前記各グループメンバはグループ公開鍵に加えてこのグループ公開鍵の更新時刻に関する情報も保持しておく。そして、前記６．のグループ認証時には双方が持つグループ公開鍵とその更新時刻の比較を行い、新しい方のグループ公開鍵で古いほうのグループ公開鍵を置き換える。

【００９９】

（３）前記２．の（４）におけるグループ情報インデックスサーバを運営している場合には、グループ情報に（１）同様グループ公開鍵の更新時刻に関する情報も含めておき、グループメンバはオンラインになった時、一定時間おき、あるいは前記６．のグループ認証を行う直前、などのタイミングで前記グループ情報インデックスサーバにアクセスして当該グループの最新のグループ公開鍵を入手する。

【０１００】

最新のグループ公開鍵に対応したグループ参加証を入手するには、グループ公開鍵の更新を検出した時点で参加証の再発行依頼（前記８．）を実行すればよい。

【０１０１】

次に、前記５．で概要を述べたグループへの新規加入依頼の処理の流れについて、図１と図２を参照して順を追って詳細に説明する。図１はグループへの新規加入を依頼する加入依頼者Ｘとグループ管理者Ａでそれぞれ実行される処理の流れを図示したものである。図２はグループへの新規加入が実行された後、加入依頼者Ｘが保持している情報を表している。

【０１０２】

［ステップ１０１］

事前に、グループ管理者Ａはグループの公開鍵ＫＧ＿Ｐ・秘密鍵ＫＧ＿Ｓのペアを作成し、このうちグループ公開鍵ＫＧ＿Ｐについては公開しておく（前記１．および前記２．を参照）。

【０１０３】

［ステップ１０２］

同じく事前に、加入依頼者Ｘは自分の公開鍵ＫＸ＿Ｐ・秘密鍵ＫＸ＿Ｓのペア

を作成しておく。これはＸが指定した情報（パスフレーズ）を元に生成されたものであってもよいし、プログラムまたは装置が生成した乱数に基づいて生成されたものであってもよい。

【０１０４】

［ステップ１０３］

Ｘは参加を所望するグループの公開鍵ＫＧ＿Ｐを入手し（前記３．参照）、またグループの管理者Ａを特定する（前記４．参照）。

【０１０５】

［ステップ１０４］

Ｘは任意の文字列Ｓを作成する。これはＸが入力した文字列そのものであってもよいし、プログラムまたは装置が生成した乱数に基づく文字列であってもよい。

【０１０６】

［ステップ１０５］

ＸはＡに文字列Ｓと自分を特定できる情報、例えば名前、住所、などを送付してグループへの新規加入を依頼する。

【０１０７】

［ステップ１０６］

ＡはＸから送られたＸを特定する情報に基づき、Ｘの加入を承認するか否かを決定する。加入を否認した場合は、Ｘがグループへ新規加入できないまま処理は終了する。

【０１０８】

［ステップ１０７］

ＡはＸから送られた文字列Ｓをグループの秘密鍵ＫＧ＿Ｓで暗号化した文字列Ｓ’＝ｅ（Ｓ，ＫＧ＿Ｓ）を作成し、Ｘに送信する。

【０１０９】

［ステップ１０８］

ＸはＡから受信したＳ’をグループ公開鍵ＫＧ＿Ｐで復号する。

【０１１０】

［ステップ１０９］

ＸはＳ’がＫＧ＿Ｐにより正常に復号され、かつその結果が元の文字列Ｓに等しいことを確認する。これにより、Ｓ’がグループ公開鍵ＫＧ＿Ｐに対応する秘密鍵ＫＧ＿Ｓによって暗号化されたこと、すなわちＡが確かにグループ秘密鍵ＫＧ＿Ｓを保持するグループ管理者であることが確認できる。復号が失敗あるいは復号結果がＳに等しくない場合はＡがグループ管理者であることが確認できないのでＸがグループへ新規加入できないまま処理は終了する。

【０１１１】

［ステップ１１０］

ＸはＡに自分の公開鍵ＫＸ＿Ｐを送信する。

【０１１２】

［ステップ１１１］

ＡはＸのグループ参加証を作成し、Ｘに送付する。グループ参加証は、Ｘの公開鍵ＫＸ＿Ｐに参加証の効果が消滅する日時Ｔ＿Ｘを添付したもの（以下”＋”で表記）をグループ秘密鍵ＫＧ＿Ｓで暗号化して作成したものであり、

Ｃ＿Ｘ＝ｅ（ＫＸ＿Ｐ＋Ｔ＿Ｘ，ＫＧ＿Ｓ）

と表せる。ＫＸ＿ＰへのＴ＿Ｘの添付方法は、両者がまとめて暗号化されていて復号前には分離不可能であり、一方復号時にはそれぞれを分離することが可能であればどのような方法であってもよい。例えばＫＸ＿Ｐ、Ｔ＿Ｘをそれぞれ文字列表現したものを所定の分離文字を介して文字列結合したものなどが考えられる。

【０１１３】

［ステップ１１２］

Ｘはグループ参加証Ｃ＿Ｘを受け取り、グループへの新規加入処理が完了する。グループへの新規加入が完了した時点でＸが保持する情報は図２に示す通りである。

【０１１４】

なお、本実施の形態では前記ステップ１０５においてＸが自分を特定できる情報を、前記ステップ１１０の時点でＸの公開鍵を、それぞれＡに対して送信する

こととしているが、これら情報は前記ステップ１０５、前記ステップ１１０のいずれであってもよいしその順序も特に限定されない。

【０１１５】

次に、前記６．で概要を説明した、参加証を獲得したＸが他のグループメンバに同じグループに属していることを認証してもらう処理の流れについて、図３を参照して順を追って詳細に説明する。図３はグループ参加証を既に入手した二人のグループ参加者Ｘとグループ参加者Ｙでそれぞれ実行される処理の流れを図示したものである。なお、Ｘは図２に示した内容の各種鍵、参加証を既に保持しているものとする。

【０１１６】

［ステップ３０１］

Ｘはグループに属している他のメンバＹのアドレス情報を特定する。それは例えば次のいずれかの方法で行われる。（１）Ｘは図１５に例示したようなＰ２Ｐネットワークの情報検索の仕組みを用いてグループを特定する情報の一部または全部をキーとして検索を行い、該当するグループに属しているユーザがこれに応答し、自分のアドレス情報をＸに対して通知する。（２）現在オンライン状態である全ユーザの少なくともアドレス情報および当該ユーザが属するグループのグループを特定する情報を収集して検索の用途に供するピア情報サーバが運営されている場合、Ｘはこのピア情報サーバに対してグループを特定する情報をキーとして検索を行い、その検索結果としてオンラインである他のグループメンバのアドレス情報を入手する。（３）他のグループメンバＹがＸにとって既知であり、かつＹが常にオンラインであってアドレス情報が変化しないことも既知である場合、そのアドレス情報を用いる。

【０１１７】

［ステップ３０２］

ＸはＹに対し認証を依頼する。

【０１１８】

［ステップ３０３］

Ｙは、前記ステップ１０４同様、任意文字列Ｓを作成しＸに送信する。

【０１１９】

［ステップ３０４］

ＸはＳを自分の秘密鍵ＫＸ＿Ｓで暗号化した文字列Ｓ’＝ｅ（Ｓ，ＫＸ＿Ｓ）を作成し、Ｓ’と自分の保持しているグループ参加証Ｃ＿ＸをＹに送信する。

【０１２０】

［ステップ３０５］

ＹはＸから送られた参加証Ｃ＿Ｘをグループ公開鍵ＫＧ＿Ｐで復号し、Ｋ＿ＸＰとＴ＿Ｘを得る。

【０１２１】

［ステップ３０６］

Ｙは前記ステップ３０５において復号が成功したことを確認する。もし失敗した場合は、参加証Ｃ＿Ｘが正しくグループ秘密鍵ＫＧ＿Ｓで暗号化されていないことを意味するので、Ｘはグループに属していないとみなされ処理は終了する。

【０１２２】

［ステップ３０７］

Ｙは前記ステップ３０５で得られた有効期限Ｔ＿Ｘが過ぎていないことを確認する。もし過ぎていれば参加証が無効であることを意味するので、Ｘはグループに属していないとみなされ処理は終了する。

【０１２３】

［ステップ３０８］

ＹはＸから送られたＳ’を前記ステップ３０５で得られたＸの公開鍵ＫＸ＿Ｐで復号する。

【０１２４】

［ステップ３０９］

Ｙは前記ステップ３０８の復号が成功し、かつ復号結果がＳと一致することを確認する。一致しなければ、Ｘは公開鍵ＫＸ＿Ｐに対応する秘密鍵ＫＸ＿Ｓを持っていないことを意味するので、Ｘは第三者の成りすましの可能性があるとみなされ処理は終了する。

【０１２５】

［ステップ３１０］

Ｙは以下のことが全て確認できたので、Ｘをグループ参加者であると認証する。（１）グループ管理者がグループ秘密鍵ＫＧ＿Ｓで暗号化したグループ参加証を保持している。（２）グループ参加証の有効期限は切れていない。（３）Ｘはグループ参加証に暗号化されていた公開鍵ＫＸ＿Ｐに対応する秘密鍵ＫＸ＿Ｓを保持している。

【０１２６】

次に、前記ステップ３０２から前記ステップ３１０までを、ＸとＹの立場を入れ替えて実行する。この処理が成功すれば、ＸはＹをグループ参加者であると認定し、相互の認定が完了する。

【０１２７】

次に、前記８．で概要を説明した、グループ参加証を更新する処理の流れについて、図４を参照して順を追って詳細に説明する。図４はグループ参加証の更新を依頼する更新依頼者Ｘとグループ管理者Ａでそれぞれ実行される処理の流れを図示したものである。なお、Ｘは図２に示した内容の各種鍵、参加証を既に保持しているものとする。

【０１２８】

［ステップ４０１］

グループ参加証を更新したいユーザＸは、グループ管理者Ａのアドレス情報を特定する（前記４．を参照）。

【０１２９】

［ステップ４０２］

Ｘは任意の文字列Ｓを作成し、Ａへ送信してグループ参加証の更新を依頼する。この文字列はＸが入力した文字列そのものであってもよいし、プログラムまたは装置が生成した乱数に基づく文字列であってもよい。

【０１３０】

［ステップ４０３］

グループ管理者ＡはＳをグループ秘密鍵ＫＧ＿Ｓで暗号化した文字列Ｓ’＝ｅ（Ｓ，ＫＧ＿Ｓ）を作成しＸへ送信する。

【０１３１】

［ステップ４０４］

ＸはＳ’をグループ公開鍵ＫＧ＿Ｐにより復号する。

【０１３２】

［ステップ４０５］

ＸはＳ’がグループ公開鍵ＫＧ＿Ｐにより正常に復号され、かつその結果が元の文字列Ｓに等しいことを確認する。これにより、Ｓ’がグループ公開鍵ＫＧ＿Ｐに対応する秘密鍵ＫＧ＿Ｓによって暗号化されたこと、すなわちＡが確かにグループ秘密鍵ＫＧ＿Ｓを保持するグループ管理者であることが確認できる。復号が失敗あるいは復号結果がＳに等しくない場合はＡがグループ管理者であることが確認できないのでＸはグループ参加証を更新することなく処理は終了する。

【０１３３】

［ステップ４０６］

ＸはＡへ自分の参加証Ｃ＿Ｘ＝ｅ（ＫＸ＿Ｐ＋Ｔ＿Ｘ，ＫＧ＿Ｓ）を送信する。

【０１３４】

［ステップ４０７］

Ａは受信したＣ＿ＸをグループＫＧ＿Ｐで復号してＫＸ＿Ｐを得る。

【０１３５】

［ステップ４０８］

Ａは前記ステップ４０７での復号が成功したことを確認する。復号に失敗した場合は、Ｘがグループ秘密鍵ＫＧ＿Ｓで暗号化されたグループ参加証を持たない、すなわちＸはグループメンバではないとみなしてＸのグループ参加証を更新することなく終了する。

【０１３６】

［ステップ４０９］

ＡはＸの公開鍵ＫＸ＿Ｐに新たな有効期限Ｔ＿Ｘ’を添付したものをグループ秘密鍵ＫＧ＿Ｓで暗号化して新たな参加証Ｃ＿Ｘ’＝ｅ（ＫＸ＿Ｐ＋Ｔ＿Ｘ’，ＫＧ＿Ｓ）を作成してＸに送信する。

【０１３７】

［ステップ４１０］

Ｘは新しい参加証Ｃ＿Ｘ’を受信する。

【０１３８】

この処理により、Ｘの参加証には新たな有効期限が添付されるのでＸはその新たな有効期限までグループに参加することができるようになる。

【０１３９】

このように、本第一の実施の形態によれば、グループ管理者が介在しなくても（オフラインであっても）、グループ管理者にグループ参加証を発行されたグループメンバ同士で互いにグループメンバであることの認証が可能となる。

【０１４０】

また、仮にグループからあるユーザを除外したい事態が発生しても、グループ参加証が有効期限を含んでいることにより、少なくともその有効期限後はそのユーザがグループメンバとして認証されないようにすることが可能となる。さらにその有効期限までの間は失効リストを参照してそのユーザをグループ認証から除外することが可能である。

【０１４１】

（実施の形態２）

前述した第一の実施の形態では、グループを構成するメンバとしては管理者と一般ユーザだけとしているが、第一の実施の形態の１０．で述べたように、グループメンバの新規加入機会を増やすためには管理者を増やす、すなわちグループ秘密鍵を複製することが必要であるが、グループ秘密鍵が複数のユーザに保持されることで、漏洩する可能性が高くなるという課題がある。

【０１４２】

本実施の形態はこれを改善するものであり、グループを構成するメンバを唯一の管理者、グループ参加証発行許可証を保持し、グループ参加証を発行する権限を持つ発行者、および一般ユーザに分類する。発行者に権限を与えることができるのは管理者のみであり、一般ユーザにグループ参加証を発行できるのは管理者および発行者である。

【０１４３】

こうすることにより、管理者が複数の発行者を設けておけば、グループの秘密鍵を複製することなくユーザの新規加入機会を増やすことが可能となる。

【０１４４】

このようなグループを管理するには、以下に示すような処理が必要となる。

【０１４５】

（１）グループの生成

（２）グループの告知

（３）グループ発行者の追加

（４）グループの発見

（５）グループ発行者の特定

（６）グループへの新規加入依頼

（７）グループメンバ間の認証

（８）グループメンバ間の情報共有

（９）グループ参加証の更新

（１０）グループ参加証発行許可証の更新

（１１）グループメンバの削除

（１２）グループ公開鍵の更新

以下、各処理について説明する。ただし第一の実施の形態と同一のものについてはその旨記して説明を省略している。

【０１４６】

１．グループの生成

第一の実施の形態の１．グループの生成と同じであるので省略する。

【０１４７】

２．グループの告知

第一の実施の形態の２．グループの告知と同じであるので省略する。

【０１４８】

３．グループ発行者の追加

前記１．でグループを生成したユーザ（グループ管理者）は、グループ参加証

発行許可証を発行することでグループメンバを追加する権限を持つユーザを必要人数追加することができる。すなわち、グループ参加証発行許可証を発行されたユーザは他のユーザに対してグループ参加証を発行することが可能となる。グループ管理者がグループ参加発行許可証を発行したユーザをグループ発行者と呼ぶ。本処理の詳細については後述する。

【０１４９】

４．グループの発見

第一の実施の形態の３．グループの発見と同じであるので省略する。

【０１５０】

５．グループ発行者の特定

あるグループへ新規加入したいユーザＸは、６．で説明するようにグループ発行者と通信する必要があり、そのために必要なグループ発行者のアドレス情報を特定する必要がある。それは例えば次のいずれかの方法で行われる。（１）Ｘは図１５に例示したようなＰ２Ｐネットワークの情報検索の仕組みを用いてグループを特定する情報の一部または全部をキーとして検索を行い、この検索要求を受けた該当するグループのグループ発行者がこれに応答し、自分のアドレス情報をＸに対して通知する。（２）現在オンライン状態である全ユーザ、あるいは少なくとも一つのグループの管理者または発行者である全ユーザの、少なくともアドレス情報および当該ユーザが管理者または発行者であるグループのグループを特定する情報を収集して検索の用途に供するピア情報サーバが運営されている場合、Ｘはこのピア情報サーバに対してグループを特定する情報をキーとして検索を行い、その検索結果として発行者のアドレス情報を入手する。（３）グループ発行者がＸにとって既知であり、かつ当該グループ発行者が常にオンラインであってアドレス情報が変化しないことも既知である場合、そのアドレス情報を用いる。

【０１５１】

６．グループへの新規加入依頼

グループへ新規加入したいユーザＸは、前記５．で特定したアドレス情報を用いてグループ発行者と通信を行い、７．で必要となるグループ参加証の発行を依

頼する。本処理の詳細については後述する。

【０１５２】

７．グループメンバ間の認証

前記６．で入手したグループ参加証を持つグループメンバ間では、互いに同じグループに属していることを認証することが可能になる。本処理の詳細については後述する。

【０１５３】

８．グループメンバ間の情報共有

第一の実施の形態の前記７．と同じであるので省略する。

【０１５４】

９．グループ参加証の更新

前記６．で発行されるグループ参加証に有効期限情報が含まれている場合には、当該有効期限以降、グループへの参加（グループメンバ間の認証）が不可能になるため、ユーザはグループ参加証の更新が必要となる。本処理の詳細については後述する。

【０１５５】

１０．グループ参加証発行許可証の更新

前記３．で発行されたグループ参加証発行許可証に有効期限情報が含まれている場合には、当該有効期限以降グループ参加証の発行が不可能になるため、発行者はグループ参加証発行許可証の更新が必要となる。本処理の詳細については後述する。

【０１５６】

１１．グループメンバの削除

第一の実施の形態同様、何らかの理由により、グループ参加証の有効期限以前に特定のメンバをグループメンバから除外したい場合がありえる。

【０１５７】

当該メンバのグループ参加証を消去する方法は、第一の実施の形態の前記９．における方法において「グループ管理者」を「グループ管理者またはグループ発行者」に置き換えた場合と同一であるので詳細な説明は省略する。第一の実施の

形態同様、失効者情報を作成・共有する方法をとることも可能である。すなわち、例えば次のような処理を実行する。

【０１５８】

（１１－１）失効者情報の作成

グループメンバの一人（グループ管理者、グループ発行者含む）が、除外されたメンバを特定する情報、例えば当該メンバの公開鍵、を含む失効者情報を作成する。

【０１５９】

（１１－２）失効者リストの共有

前記７．のグループメンバ間の認証の際には、自分が保持する失効者情報のリストと認証相手が持つ失効者情報のリストを比較し、一方のリストに含まれない失効者情報が存在する場合は互いに他方のリストに追加することで、失効者情報のリストを全グループメンバで共有するようにする。

【０１６０】

（１１－３）失効者の除外

前記７．のグループメンバ間の認証の際に、認証相手が自分の保持する失効者情報のリストに含まれているかどうかを確認し、含まれている場合は相手をグループメンバであると認証しない。例えばユーザの公開鍵を失効者情報として用いる場合は、認証相手の公開鍵がリストに含まれる失効者情報のいずれかと一致すれば、この相手の認証を拒否する。

【０１６１】

（１１－４）失効者の参加資格更新の拒否

前記９．においてグループ参加証の更新を行う際に、参加証の更新を依頼したユーザがリストに含まれる失効者情報のいずれかと一致するかどうかを確認し、一致するものがある場合は参加証の更新を拒否する。

【０１６２】

なお、失効ユーザ情報にその消去期限を含めておいて、消去期限を越えた失効者情報を削除することが可能であるのは第一の実施の形態同様である。

【０１６３】

また、第一の実施の形態同様、失効者情報の作成はグループ発行者のみが行い、グループ発行者が自分の秘密鍵を用いて暗号化した状態で共有することとしてもよい。グループメンバは失効者情報とそれを発行したグループ発行者の参加証発行許可証を同時に入手することにより、この参加証発行許可証に含まれるグループ発行者の公開鍵を用いて失効者情報を復号することが可能であり、この失効者情報が不正に改ざんされていないことの確認が可能となる。これにより、悪意を持つユーザにより作成された不正な失効者情報が共有されることを防ぐことができる。

【０１６４】

１２．グループ公開鍵の更新

何らかの事故によりグループ秘密鍵ＫＧ＿Ｓがグループ管理者以外のユーザに漏洩した場合、グループ秘密鍵を入手したユーザは不正にグループ参加証発行許可証を発行することが可能となり、ひいてはグループ参加証を不正に発行することが可能となる。このときグループメンバには不正なグループ参加証発行許可証やグループ参加証と正規のものを判別することはできない。このような場合には、グループ公開鍵・秘密鍵のペアを更新する以外に不正を防ぐ方法はない。一方、グループ管理者がグループ公開鍵・秘密鍵をそれぞれＫＧ＿Ｐ’、ＫＧ＿Ｓ’に更新したとしても、従来のグループ公開鍵ＫＧ＿Ｐとそれに基づいて作成されたグループ参加証発行許可証を持つグループメンバ同士では前記６．のグループ認証は互いに可能なままなので、グループメンバは常に最新のグループ公開鍵を保持しておく必要があると同時に、最新のグループ公開鍵に対応したグループ参加証を入手する必要がある。発行者はこれに加えて最新のグループ鍵に対応したグループ参加証発行許可証を入手する必要がある。

【０１６５】

最新のグループ公開鍵の保持は、第一の実施の形態同様、例えば次のいずれかのような方法により可能である。

【０１６６】

（１）グループ管理者がグループ公開鍵・秘密鍵を更新した時点で、図１５に例示したようなＰ２Ｐネットワークを介してネットワーク参加者全員に新しいグ

ループ公開鍵を送付する。対応するグループのメンバは、この新しいグループ公開鍵で自分が保持しているグループ公開鍵を置き換える。

【０１６７】

（２）前記２．で告知されるグループ情報に、グループ公開鍵の更新時刻に関する情報も含めておき、前記各グループメンバはグループ公開鍵に加えてこのグループ公開鍵の更新時刻に関する情報も保持しておく。そして、前記６．のグループ認証時には双方が持つグループ公開鍵とその更新時刻の比較を行い、新しい方のグループ公開鍵で古いほうのグループ公開鍵を置き換える。

【０１６８】

（３）前記２．の（４）におけるグループ情報インデックスサーバを運営している場合には、グループ情報に（１）同様グループ公開鍵の更新時刻に関する情報も含めておき、グループメンバはオンラインになった時、一定時間おき、あるいは前記６．のグループ認証を行う直前、などのタイミングで前記グループ情報インデックスサーバにアクセスして当該グループの最新のグループ公開鍵を入手する。

【０１６９】

最新のグループ公開鍵に対応したグループ参加証発行許可証を入手するには、グループ公開鍵の更新を検出した時点で参加証の再発行依頼（前記１０．）を実行すればよい。

【０１７０】

最新のグループ公開鍵に対応したグループ参加証を入手するには、グループ公開鍵の更新を検出した時点で参加証の再発行依頼（前記１０．）を実行すればよい。

【０１７１】

次に、前記３．で概要を説明したグループ発行者の追加処理の流れについて、図５と図６を参照して順を追って詳細に説明する。図５はグループ管理者Ａとグループ発行者Ｂでそれぞれ実行される処理の流れを図示したものである。図６はグループ発行者の追加処理が終了した後、グループ発行者が保持する情報を表している。

【０１７２】

［ステップ５０１］

事前に、グループ管理者Ａはグループの公開鍵ＫＧ＿Ｐ・秘密鍵ＫＧ＿Ｓのペアを作成し、このうちグループ公開鍵ＫＧ＿Ｐについては公開しておく。

【０１７３】

［ステップ５０２］

同じく事前に、発行者候補ＢＸは自分の公開鍵ＫＢ＿Ｐ・秘密鍵ＫＢ＿Ｓのペアを作成しておく。これはＢが指定した情報（パスフレーズ）を元に生成されたものであってもよいし、プログラムまたは装置が生成した乱数に基づいて生成されたものであってもよい。

【０１７４】

［ステップ５０３］

グループ管理者Ａは追加するグループ発行者としてユーザＢを選択し、Ｂのアドレス情報を特定する。それは例えば次のような方法で行われる。（１）図１５で図示されるＰ２Ｐネットワークの情報検索の仕組みを用いて当該グループに参加しているユーザを検索し、該当するユーザがＡに対して自分個人を特定する情報と自分のアドレス情報を返信する。Ａは受信した情報から、適切と判断するユーザを選択する。（２）電子メールなどＰ２Ｐネットワーク以外の手段を含む何らかの手段でＢに対してグループ発行者になることを依頼し、Ｂがそれを受け入れる場合はＡに対して自分のアドレス情報を返信する。

【０１７５】

［ステップ５０４］

ＡはＢに対してＢの公開鍵を送信するよう要求する。

【０１７６】

［ステップ５０５］

ＢはＡに対して自分の公開鍵ＫＢ＿Ｐを送信する。

【０１７７】

［ステップ５０６］

ＡはＢの公開鍵ＫＢ＿Ｐに有効期限情報Ｔ＿Ｂを添付したものをグループの秘

密鍵で暗号化してグループ参加証許可証Ｉ＿Ｂ＝ｅ（ＫＢ＿Ｐ＋Ｔ＿Ｂ，ＫＧ＿Ｓ）を作成し、Ｂに送信する。

【０１７８】

［ステップ５０７］

Ｂはグループ参加証許可証Ｉ＿Ｂを受け取る。

【０１７９】

これにより、Ｂは他ユーザに対してグループ参加証を発行することが可能になる。本処理後Ｂが保持する情報は図６に示す通りである。

【０１８０】

なお、本実施の形態ではグループ管理者ＡがＢに対しグループ発行者の権限を持つよう依頼することとしているが、逆にＢの方からグループ発行者の権限をＡに対して要求し、Ａがそれを承認する形で処理を進めても良い。その場合は、上記ステップ５０３はＢの方からアドレス情報をＡに対して通知する処理となる。

【０１８１】

次に、前記６．で概要を説明したグループへの新規加入依頼処理の流れについて、図７と図８を参照して順を追って詳細に説明する。図７はグループへの新規加入を依頼する加入依頼者Ｘとグループ発行者Ｂでそれぞれ実行される処理の流れを図示したものである。図８はグループへの新規加入依頼処理が終了した後、Ｘが保持する情報を表している。なお、グループ発行者Ｂは図６に示す情報を保持しているものとする。

【０１８２】

［ステップ７０１］

Ｘは参加を所望するグループの公開鍵ＫＧ＿Ｐを入手し（前記４．参照）、またグループ発行者Ｂを特定する（前記５．参照）。

【０１８３】

［ステップ７０２］

Ｘは任意の文字列Ｓを作成し、Ｂに送信してグループへの新規加入を依頼する。ＳはＸが入力した文字列そのものであってもよいし、プログラムまたは装置が生成した乱数に基づく文字列であってもよい。

【０１８４】

［ステップ７０３］

ＢはＳを自分の秘密鍵ＫＢ＿Ｓで暗号化したＳ’＝ｅ（Ｓ，ＫＢ＿Ｓ）とグループ参加証発行許可証Ｉ＿ＢをＸへ送信する。

【０１８５】

［ステップ７０４］

ＸはＩ＿Ｂをグループ公開鍵ＫＧ＿Ｐで復号し、Ｂの公開鍵ＫＢ＿Ｐと有効期限Ｔ＿Ｂを得る。

【０１８６】

［ステップ７０５］

ＸはＩ＿ＢがＫＧ＿Ｐにより正常に復号されたことを確認する。正常に復号されない場合は、Ｂの持つグループ参加証発行許可証Ｉ＿ＢがグループＫＧ＿Ｓで暗号化したものであること、すなわちＢがグループ発行者であることが確認できないのでＸはグループへ新規加入しないまま処理を終了する。

【０１８７】

［ステップ７０６］

Ｘは次いでＳ’をＢの公開鍵ＫＢ＿Ｐで復号する。

【０１８８】

［ステップ７０７］

ＸはＳ’がＫＢ＿Ｐにより正常に復号され、かつその結果が元の文字列Ｓに等しいことを確認する。これにより、Ｓ’がの公開鍵ＫＢ＿Ｐに対応する秘密鍵ＫＢ＿Ｓによって暗号化されたこと、すなわちＢが確かに秘密鍵ＫＢ＿Ｓを保持するグループ管理者であることが確認できる。復号が失敗あるいは復号結果がＳに等しくない場合はＢがグループ発行者であることが確認できないのでＸはグループへ新規加入しないまま処理は終了する。

【０１８９】

［ステップ７０８］

ＸはＢに自分の公開鍵ＫＸ＿Ｐを送信する。

【０１９０】

［ステップ７０９］

ＢはＸのグループ参加証を作成し、Ｘに送付する。参加証は、Ｘの公開鍵ＫＸ＿Ｐに参加証の効果が消滅する日時Ｔ＿Ｘを添付したもの（以下”＋”で表記）をＢの秘密鍵ＫＢ＿Ｓで暗号化して作成したものであり、

Ｃ＿Ｘ＝ｅ（ＫＸ＿Ｐ＋Ｔ＿Ｘ，ＫＢ＿Ｓ）

と表せる。ＫＸ＿ＰへのＴ＿Ｘの添付方法は、両者がまとめて暗号化されていて復号前には分離不可能であり、一方復号時にはそれぞれを分離することが可能であればどのような方法であってもよい。例えばＫＸ＿Ｐ、Ｔ＿Ｘをそれぞれ文字列表現したものを所定の分離文字を介して文字列結合したものなどが考えられる。

【０１９１】

［ステップ７１０］

Ｘはグループ参加証Ｃ＿Ｘを受け取り、グループへの新規加入処理が完了する。グループへの新規加入が完了した時点でＸが保持する情報は図８に示す通りである。

【０１９２】

なお、本実施の形態では前記ステップ７０８においてＸの公開鍵をＢに対して送信することとしているが、これは前記ステップ７０２の時点で送信してもよい。

【０１９３】

また、第一の実施の形態におけるグループへの新規加入依頼同様、前記ステップ７０２の時点でＸがＢに対して自分個人を特定できる情報も加えて送信し、Ｂはその個人を特定できる情報に基づいてＸを加入させるかどうか判断し、加入させない場合はＸを加入させることなく処理を終了することとしてもよい。

【０１９４】

次に、前記７．で概要を説明したグループメンバ間の認証処理の流れについて、図１０を参照して順を追って詳細に説明する。図１０はグループ参加証を既に入手した二人のグループ参加者Ｘとグループ参加者Ｙでそれぞれ実行される処理

の流れを図示したものである。なお、ＸとＹはそれぞれ図８と図９に示す情報を保持しているものとする。

【０１９５】

ステップ１００１およびステップ１００２は第一の実施の形態における前記ステップ３０１および前記ステップ３０２と同様であるので詳しい説明は省略する。

【０１９６】

［ステップ１００３］

Ｘは、Ｓを自分の秘密鍵ＫＸ＿Ｓで暗号化した文字列Ｓ’＝ｅ（Ｓ，ＫＸ＿Ｓ）を作成し、Ｓ’、グループ発行者から受け取ったグループ参加証発行証明書Ｉ＿Ｂおよびグループ参加証Ｃ＿ＸをＹに送信する。

【０１９７】

［ステップ１００４］

Ｙは、グループ参加証発行証明書Ｉ＿Ｂをグループ公開鍵ＫＧ＿Ｐで復号し、グループ発行者の公開鍵ＫＢ＿Ｐおよびグループ参加証発行証明書の有効期限Ｔ＿Ｂを得る。

【０１９８】

［ステップ１００５］

Ｙは、前記ステップ１００４で復号が成功したことおよび得られた有効期限Ｔ＿Ｂが過ぎていないことを確認する。復号が失敗した場合はグループ参加証発行許可証が正しくグループ秘密鍵ＫＧ＿Ｓで暗号化されていないことを意味し、また有効期限が過ぎていればグループ参加証発行許可証が無効であることを意味するので、いずれもＸはグループに属していないとみなされ処理は終了する。

【０１９９】

［ステップ１００６］

Ｙは、Ｘのグループ参加証Ｃ＿ＸをグループＸ発行者の公開鍵ＫＢ＿Ｐで復号し、Ｘの公開鍵ＫＸ＿ＰおよびＸのグループ参加証の有効期限Ｔ＿Ｘを得る。

【０２００】

［ステップ１００７］

Ｙは、前記ステップ１００６で復号が成功したことおよび得られた有効期限Ｔ＿Ｘが過ぎていないことを確認する。復号が失敗した場合はグループ参加証がグループ発行者の秘密鍵ＫＢ＿Ｓで暗号化されていないことを意味し、また有効期限が過ぎていればグループ参加証が無効であることを意味するので、いずれもＸはグループに属していないとみなされ処理は終了する。

【０２０１】

［ステップ１００８］

次にＹは、Ｓ’をＸの公開鍵ＫＸ＿Ｐで復号する。

【０２０２】

［ステップ１００９］

Ｙは、前記ステップ１００８で復号が成功したことおよび復号結果がＳに一致することを確認する。復号が失敗した場合および復号結果がＳに一致しない場合はＸが公開鍵ＫＸ＿Ｐに対応する秘密鍵ＫＸ＿Ｓを持っていないことを意味するので、Ｘは第三者の成りすましの可能性があるとみなされ処理は終了する。

【０２０３】

［ステップ１０１０］

Ｙは以下のことが全て確認できたので、Ｘをグループ参加者であると認証する。（１）グループ参加証の有効期限は切れていない。（２）Ｘはグループ参加証に暗号化されていた公開鍵ＫＸ＿Ｐに対応する秘密鍵ＫＸ＿Ｓを保持している。（３）グループ参加証を発行したグループ発行者のグループ参加証発行証明書の有効期限は切れていない。（４）グループ参加証を発行したグループ発行者は、グループ参加証発行証明書に暗号化されていた公開鍵ＫＢ＿Ｐに対応する秘密鍵ＫＢ＿Ｓを保持している。（５）グループ参加証発行証明書は、グループ管理者によってグループ秘密鍵ＫＧ＿Ｓによって暗号化されたものである。

【０２０４】

次に、前記ステップ１００２から前記ステップ１０１０までを、ＸとＹの立場を入れ替えて実行する。この処理が成功すれば、ＸはＹをグループ参加者であると認定し、相互の認定が完了する。

【０２０５】

次に、前記９．で概要を説明したグループ参加証の更新処理の流れについて、図１１と図１２を参照して順を追って詳細に説明する。図１１はグループ参加証の更新を依頼する参加証更新依頼者Ｘとグループ発行者Ｂでそれぞれ実行される処理の流れを図示したものである。図１２はグループ参加証の更新処理が終了した後、Ｘが保持する情報を表している。なお、Ｘは事前に図８に示す情報を、Ｂは図６に示す情報を保持しているものとする。

【０２０６】

［ステップ１１０１］

Ｘはグループ発行者Ｂを特定する（前記５．参照）。なお、ここではグループ発行者としてＢを特定したが、同じグループのグループ発行者であれば誰であっても以降の処理は成立する。

【０２０７】

ステップ１１０２～ステップ１１０８は前記ステップ７０２～前記ステップ７０８と同一であるので説明を省略する。

【０２０８】

［ステップ１１０９］

ＢはＸの新たなグループ参加証を作成し、Ｘに送付する。すなわち、Ｘの公開鍵ＫＸ＿Ｐに新たな有効期限Ｔ＿Ｘ’を添付したものをＢの秘密鍵ＫＢ＿Ｓで暗号化して作成したＣ＿Ｘ’＝ｅ（ＫＸ＿Ｐ＋Ｔ＿Ｘ’，ＫＢ＿Ｓ）が新たなグループ参加証となる。

【０２０９】

［ステップ１１１０］

Ｘは更新されたグループ参加証Ｃ＿Ｘ’を受け取り、グループ参加証の更新処理が完了する。グループ参加証の更新処理が完了した時点でＸが保持する情報は図１２に示す通りである。

【０２１０】

次に、前記１０．で概要を説明したグループ参加証発行許可証の更新処理の流れについて、図１３と図１４を参照して順を追って詳細に説明する。図１３はグループ参加証発行許可証の更新を依頼するグループ発行者Ｂとグループ管理者Ａ

でそれぞれ実行される処理の流れを図示したものである。図１４はグループ参加証発行許可証の更新が終了した後、Ｂが保持する情報を表している。

【０２１１】

［ステップ１３０１］

グループ発行者ＢはグループＡを特定する。第一の実施の形態の処理４．で例示した方法と同じ方法で行われる。

【０２１２】

［ステップ１３０２］

Ｂは任意の文字列Ｓを作成し、Ａへ送付して参加証発行許可証の更新を依頼する。ＳはＢが入力した文字列そのものであってもよいし、プログラムまたは装置が生成した乱数に基づく文字列であってもよい。

【０２１３】

［ステップ１３０３］

ＡはＳをグループ秘密鍵ＫＧ＿Ｓで暗号化したＳ’＝ｅ（Ｓ，ＫＧ＿Ｓ）を作成しＢへ送信する。

【０２１４】

［ステップ１３０４］

ＢはＳ’をグループ公開鍵ＫＧ＿Ｐで復号する。

【０２１５】

［ステップ１３０５］

ＢはＳ’がＫＧ＿Ｐにより正常に復号され、かつその結果が元の文字列Ｓに等しいことを確認する。これにより、Ｓ’がグループ公開鍵ＫＧ＿Ｐに対応する秘密鍵ＫＧ＿Ｓによって暗号化されたこと、すなわちＡが確かにグループ秘密鍵ＫＧ＿Ｓを保持するグループ管理者であることが確認できる。復号が失敗あるいは復号結果がＳに等しくない場合はＡがグループ管理者であることが確認できないので、Ｂはグループ参加証発行許可証を更新することなく処理は終了する。

【０２１６】

［ステップ１３０６］

ＢはＡへ自分の保持するグループ参加証発行許可証Ｉ＿Ｂを送信する。

【０２１７】

［ステップ１３０７］

ＡはＩ＿Ｂをグループ公開鍵ＫＧ＿Ｐで復号し、Ｂの公開鍵ＫＢ＿Ｐを得る。

【０２１８】

［ステップ１３０８］

Ａは前記ステップ１３０７で復号が成功したことを確認する。復号が成功した場合は、Ｂが持つグループ参加証発行許可証がグループ秘密鍵ＫＧ＿Ｓで暗号化されたものであること、すなわちＢが正当なグループ発行者であることが確認できる。復号が失敗した場合は、Ｂが正当なグループ発行者であることを確認できないのでＢのグループ参加証発行許可証は更新されないまま処理は終了する。

【０２１９】

［ステップ１３０９］

ＡはＢの公開鍵ＫＢ＿Ｐを新たな有効期限Ｔ＿Ｂ’と共にグループ秘密鍵ＫＧ＿Ｓで暗号化して更新されたグループ参加証発行許可証Ｉ＿Ｂ’＝ｅ（ＫＢ＿Ｐ＋Ｔ＿Ｂ’，ＫＧ＿Ｓ）を作成し、Ｂに送信する。

【０２２０】

［ステップ１３１０］

Ｂは更新されたグループ参加証発行許可証Ｉ＿Ｂ’を受け取る。この時点でＢが保持する情報は図１４に示す通りである。

【０２２１】

なお、本実施の形態において、グループ参加証発行証明書には有効期限をもうけているが、さらに前記処理１１．で述べたグループメンバの失効者情報同様、グループ発行者の失効情報を作成・共有・除外および許可証更新の拒否を行うことで、あるグループ発行者の参加証発行権限を直ちに剥奪することも可能である。

【０２２２】

本第二の実施の形態独自の効果としては、グループ参加証を発行できるグループ発行者をグループ管理者が必要に応じて設けることにより、秘匿性の高いグループ秘密鍵を複製することなくユーザのグループへの新規加入の機会を増やすこ

とができる点があげられる。

【０２２３】

なお、第一及び第二の実施の形態では、グループ参加証、グループ参加証発行許可証、あるいは失効リストをグループ管理者あるいはグループ発行者の秘密鍵で暗号化することとしているが、暗号化される内容は公開されている公開鍵および有効期限情報などであって必ずしも秘匿すべき内容ではないので、暗号化する代わりに前記秘密鍵で署名を行うこととしてもよい。この場合でも、受信者は内容の改ざんるいは不正な発行を検出することができるので、本発明の効果には影響がない。

【０２２４】

また、第一，第二の実施の形態共に参加証に添付する有効期限は参加証の効果が消滅する日時を示すものとしたが、参加証には参加証の発行日時を添付しておき、有効期限を確認する前記ステップ３０７では現在日時と発行日時の差分を取り、所定の期間、例えば１ヶ月、を超えていなければ有効期限内であると判断する方法でもよい。

【０２２５】

さらに、有効期限の判定に利用される現在日時は通常装置のクロックから取り出されるが、グループ認証を行う二ユーザのそれぞれのクロックが大きく乖離しているとグループ認証処理に影響を及ぼす可能性があるので、双方のクロックが大きくずれた状態でグループ認証処理を行うことは望ましくない。この課題に対しては、グループ認証を行う前に互いのクロックを比較し、所定の基準より大きくずれている場合にはユーザに対して警告を発してグループ認証処理を行わない方法、あるいはどちらか一方のクロックに強制的に他方のクロックを合わせる方法、あるいは双方のクロックの平均値を取って双方ともそれに合わせる方法、などにより対処することが考えられる。

【０２２６】

さらに、第一の実施の形態の前記処理７．および第二の実施の形態の前記処理８．以外においては通信路の暗号化について言及していないが、全処理について第一の実施の形態の前記処理７．と同様情報転送の暗号化処理を施してもよい。

やり取りされるグループ参加証やグループ参加証発行許可証などは、それを第三者が入手してもメンバあるいはグループ発行者の秘密鍵をも入手しない限りは直ちに不正使用することはできないためこの暗号化処理は必須ではないが、よりセキュリティを高めるために通信路の暗号化を導入することは可能である。

【０２２７】

さらに、複数のグループ公開鍵・グループ秘密鍵のペアを作成・保持することにより、同一ユーザが複数のグループの管理者となることが可能であるのは言うまでもない。同様に複数グループのそれぞれの参加証あるいは参加証発行許可証を保持することにより、同一ユーザが複数グループのそれぞれメンバあるいは発行者となることが可能であるし、同一ユーザが複数のグループに対して異なる権限を持つメンバすなわち管理者・発行者・一般メンバのいずれかとして属することも可能である。

【０２２８】

【発明の効果】

本発明によれば、以下の利点を持つネットワーク上のグループ管理が可能となる。すなわち、（１）常時稼動しているサーバの運用が不要であり、（２）グループ管理者を含む各グループメンバのオンライン・オフライン状態によらず、グループメンバ間で互いにグループメンバであることの認証が常に可能である。これにより、グループでのみ共有している情報をグループ外のメンバへ漏洩する恐れなく安全に共有することが可能になる。

【図面の簡単な説明】

【図１】

第一の実施の形態におけるグループへの新規加入処理の流れを示した図

【図２】

第一の実施の形態においてグループ参加者Ｘが保持している情報を示した図

【図３】

第一の実施の形態におけるグループ参加者同士による認証処理の流れを示した図

【図４】

第一の実施の形態におけるグループ参加証の更新処理の流れを図示した図

【図５】

第二の実施の形態におけるグループ発行者の追加処理の流れを図示した図

【図６】

第二の実施の形態においてグループ発行者Ｂが保持する情報を示した図

【図７】

第二の実施の形態におけるグループへの新規加入処理の流れを図示した図

【図８】

第二の実施の形態においてグループ参加者Ｘが保持している情報を示した図

【図９】

第二の実施の形態においてグループ参加者Ｙが保持している情報を示した図

【図１０】

第二の実施の形態におけるグループ参加者同士で行われる認証処理の流れを示した図

【図１１】

第二の実施の形態におけるグループ参加証の更新処理の流れを示した図

【図１２】

第二の実施の形態においてグループ参加証を更新したグループ参加者Ｘが保持している情報を示した図

【図１３】

第二の実施の形態におけるグループ参加証発行許可証の更新処理の流れを示した図

【図１４】

第二の実施の形態においてグループ参加証発行許可証を更新したグループ発行者Ｂが保持している情報を示した図

【図１５】

Ｐ２Ｐネットワークに参加しているユーザ間での情報転送の流れを表した概念図

【図１６】

Ｐ２Ｐネットワークにおけるグループ管理の問題点を表した図

【符号の説明】

１０１～１１２　第一の実施の形態におけるグループへの新規加入処理の各ステップ

３０１～３１０　第一の実施の形態におけるグループ参加者同士による認証処理の各ステップ

４０１～４１０　第一の実施の形態におけるグループ参加証の更新処理の各ステップ

５０１～５０７　第二の実施の形態におけるグループ発行者の追加処理の各ステップ

７０１～７１０　第二の実施の形態におけるグループへの新規加入処理の各ステップ

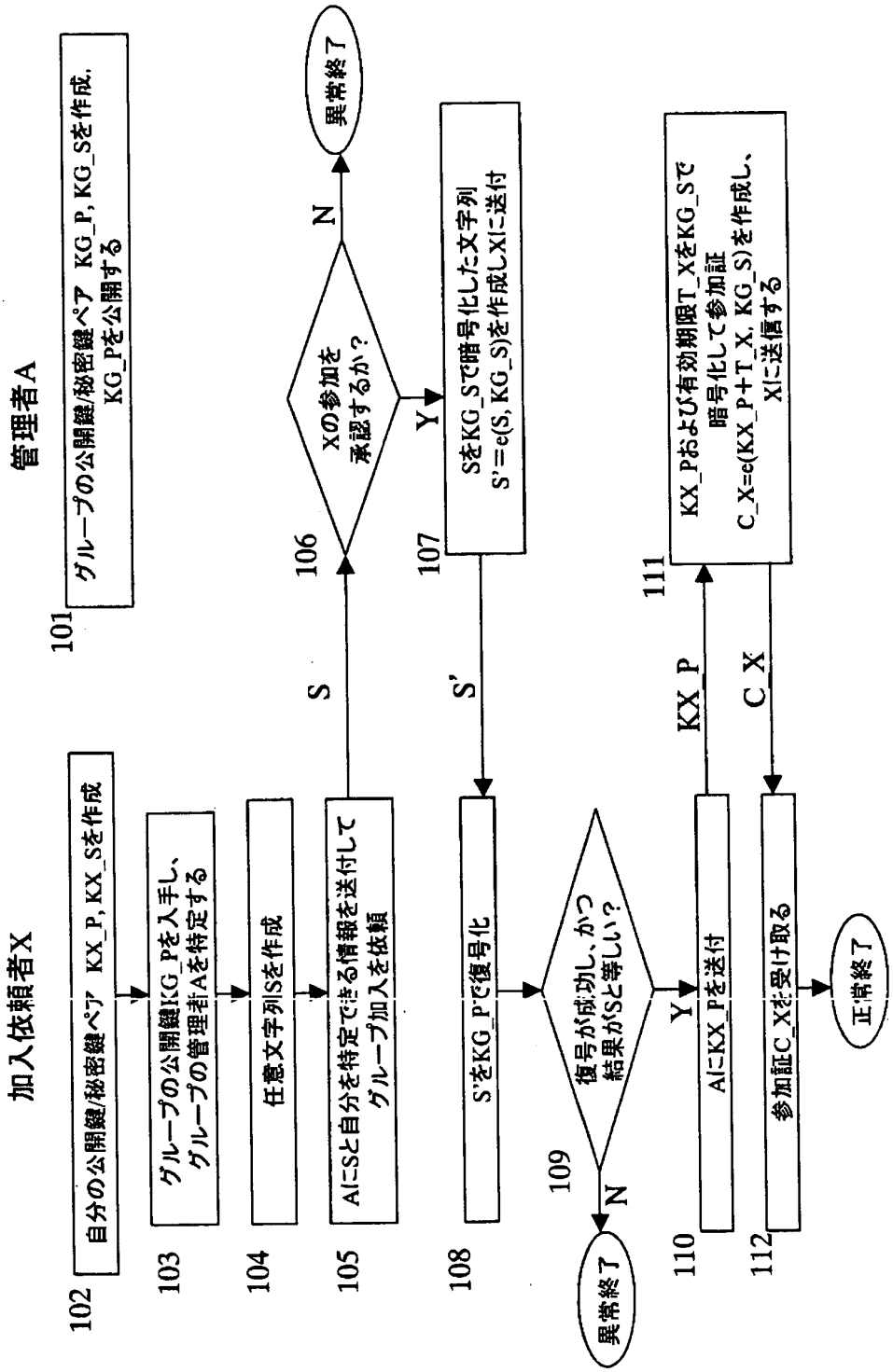
１００１～１０１０　第二の実施の形態におけるグループ参加者同士による認証処

１１０１～１１１０　第二の実施の形態におけるグループ参加証の更新処理の各ス

１３０１～１３１０　第二の実施の形態におけるグループ参加証発行許可証の更新処理の各ステップ

【書類名】　図面

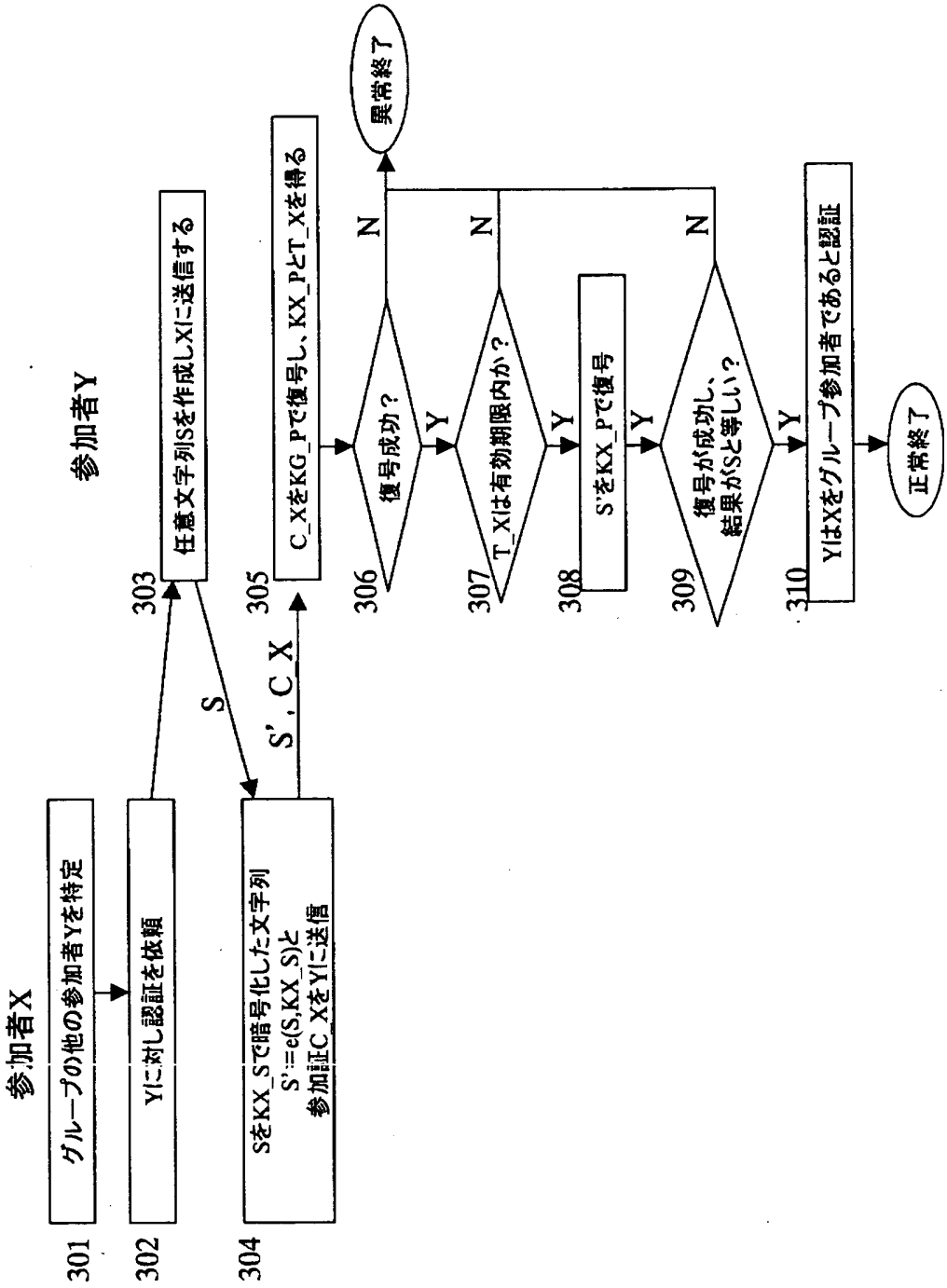
【図１】


管理者A
加入依頼者X
101 グループの公開鍵/秘密鍵ペア KG_P, KG_Sを作成, KG_Pを公開する
102 自分の公開鍵/秘密鍵ペア KX_P, KX_Sを作成
103 グループの公開鍵KG_Pを入手し、グループの管理者Aを特定する
104 任意文字列Sを作成
105 AにSと自分を特定できる情報を送付してグループ加入を依頼
106 Xの参加を承認するか？
N
異常終了
S
Y
107 SをKG_Sで暗号化した文字列 S'=e(S, KG_S)を作成しXに送付
S'
108 S'をKG_Pで復号化
109 復号が成功し、かつ結果がSと等しい？
N
異常終了
Y
110 AにKX_Pを送付
KX_P
111 KX_Pおよび有効期限T_XをKG_Sで暗号化して参加証 C_X=e(KX_P+T_X, KG_S)を作成し、Xに送信する
C_X
112 参加証C_Xを受け取る
正常終了

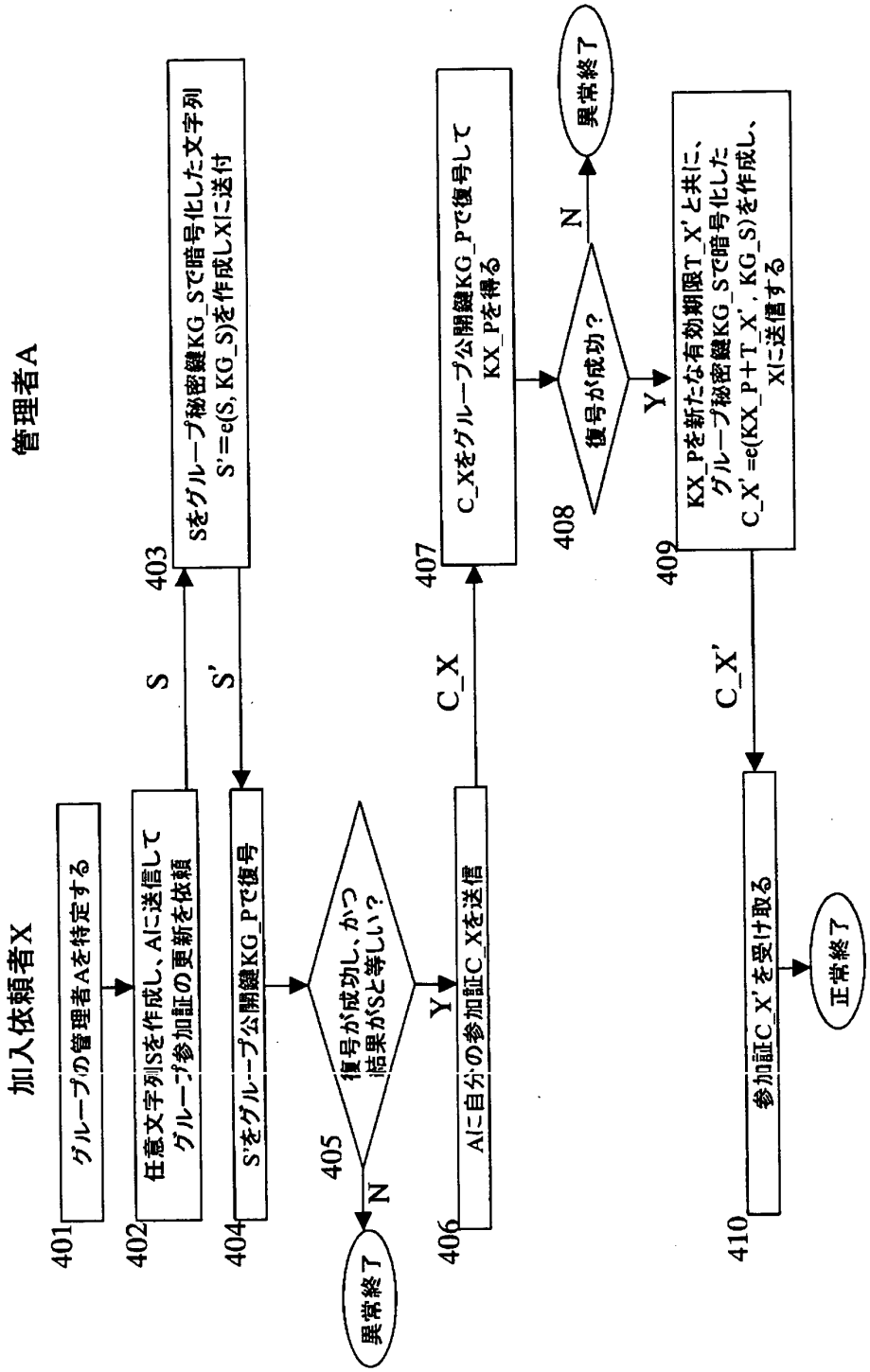
【図２】

KX_P:Xの公開鍵
KX_S:Xの秘密鍵
KG_P:グループの公開鍵
C_X=e(KX_P+T_X,KG_S):Xのグループ参加証

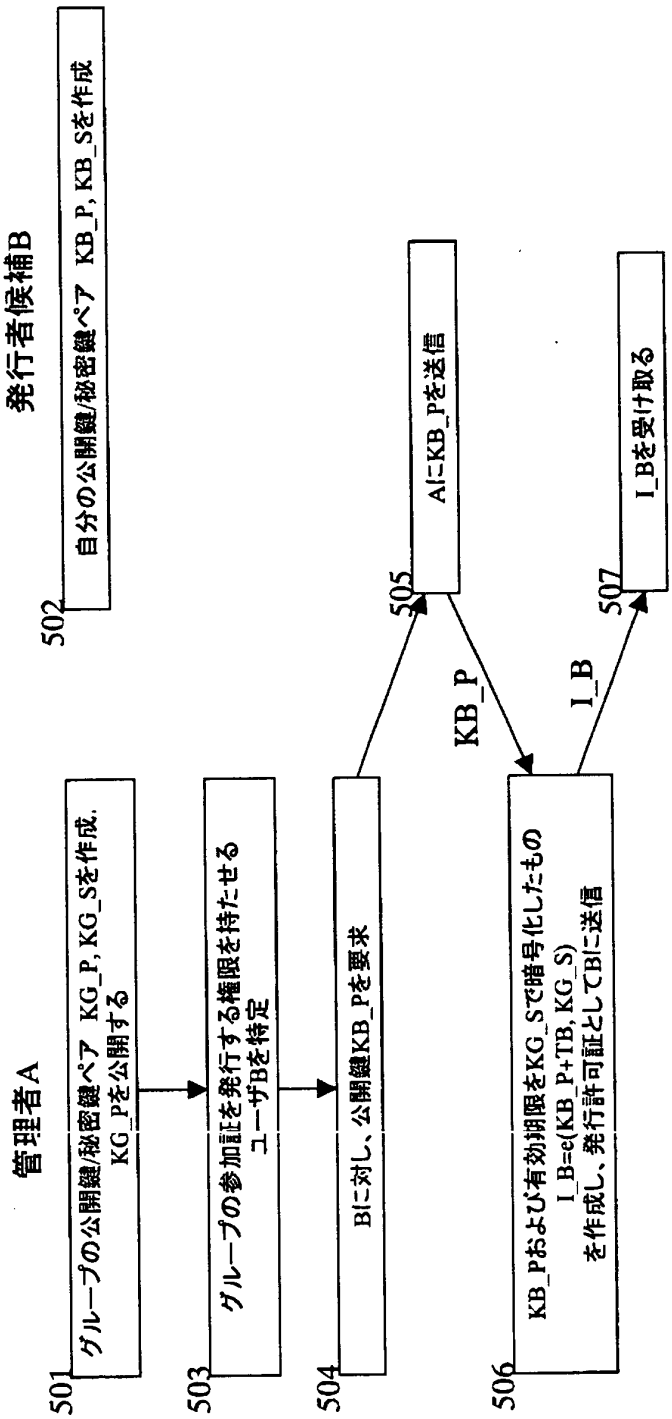
【図３】


参加者X
参加者Y
グループの他の参加者Yを特定
301
Yに対し認証を依頼
302
任意文字列Sを作成しXに送信する
303
S
SをKX_Sで暗号化した文字列
S'=e(S,KX_S)と
参加証C_XをYに送信
304
S', C X
C_XをKG_Pで復号し、KX_PとT_Xを得る
305
異常終了
復号成功？
306
N
Y
T_Xは有効期限内か？
307
N
Y
S'をKX_Pで復号
308
Y
復号が成功し、
結果がSと等しい？
309
N
Y
YはXをグループ参加者であると認証
310
正常終了

【図４】


管理者A
加入依頼者X
401
グループの管理者Aを特定する
402
任意文字列Sを作成し、Aに送信して
グループ参加証の更新を依頼
S
403
Sをグループ秘密鍵KG_Sで暗号化した文字列
S'=e(S, KG_S)を作成しXに送付
S'
404
S'をグループ公開鍵KG_Pで復号
405
復号が成功し、かつ
結果がSと等しい？
N
異常終了
Y
C_X
406
Aに自分の参加証C_Xを送信
407
C_Xをグループ公開鍵KG_Pで復号して
KX_Pを得る
408
復号が成功？
N
異常終了
Y
409
KX_Pを新たな有効期限T_X'と共に、
グループ秘密鍵KG_Sで暗号化した
C_X'=e(KX_P+T_X', KG_S)を作成し、
Xに送信する
C_X'
410
参加証C_X'を受け取る
正常終了

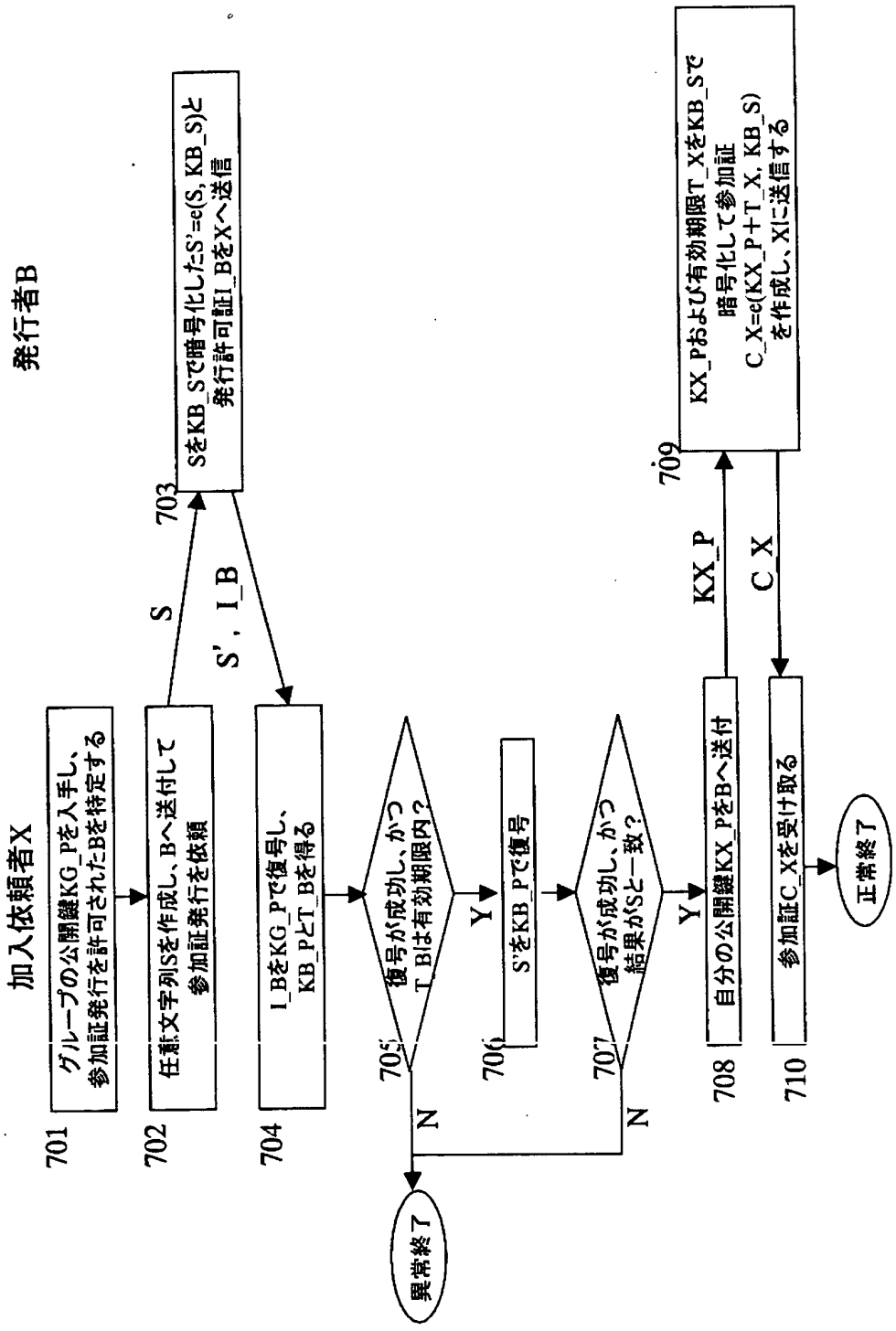
【図５】


管理者A
発行者候補B
501
グループの公開鍵/秘密鍵ペア KG_P, KG_Sを作成.
KG_Pを公開する
503
グループの参加証を発行する権限を持たせる
ユーザBを特定
504
Bに対し、公開鍵KB_Pを要求
502
自分の公開鍵/秘密鍵ペア KB_P, KB_Sを作成
505
AにKB_Pを送信
KB_P
506
KB_Pおよび有効期限をKG_Sで暗号化したもの
I_B=e(KB_P+TB, KG_S)
を作成し、発行許可証としてBに送信
I_B
507
I_Bを受け取る

【図６】

KB_P:Bの公開鍵
KB_S:Bの秘密鍵
KG_P:グループの公開鍵
I_B=e(KB_P+T_B,KG_S)
:Bのグループ参加証発行許可証

【図７】


加入依頼者X
発行者B
グループの公開鍵KG_Pを入手し、参加証発行を許可されたBを特定する
701
任意文字列Sを作成し、Bへ送付して参加証発行を依頼
702
S
S', I_B
SをKB_Sで暗号化したS'=e(S, KB_S)と発行許可証I_BをXへ送信
703
I_BをKG_Pで復号し、KB_PとT_Bを得る
704
復号が成功し、かつT_Bは有効期限内？
705
Y
N
異常終了
S'をKB_Pで復号
706
復号が成功し、かつ結果がSと一致？
707
Y
N
自分の公開鍵KX_PをBへ送付
708
KX_P
KX_PおよびT_XをKB_Sで暗号化して参加証C_X=e(KX_P+T_X, KB_S)を作成し、Xに送信する
709
C_X
参加証C_Xを受け取る
710
正常終了

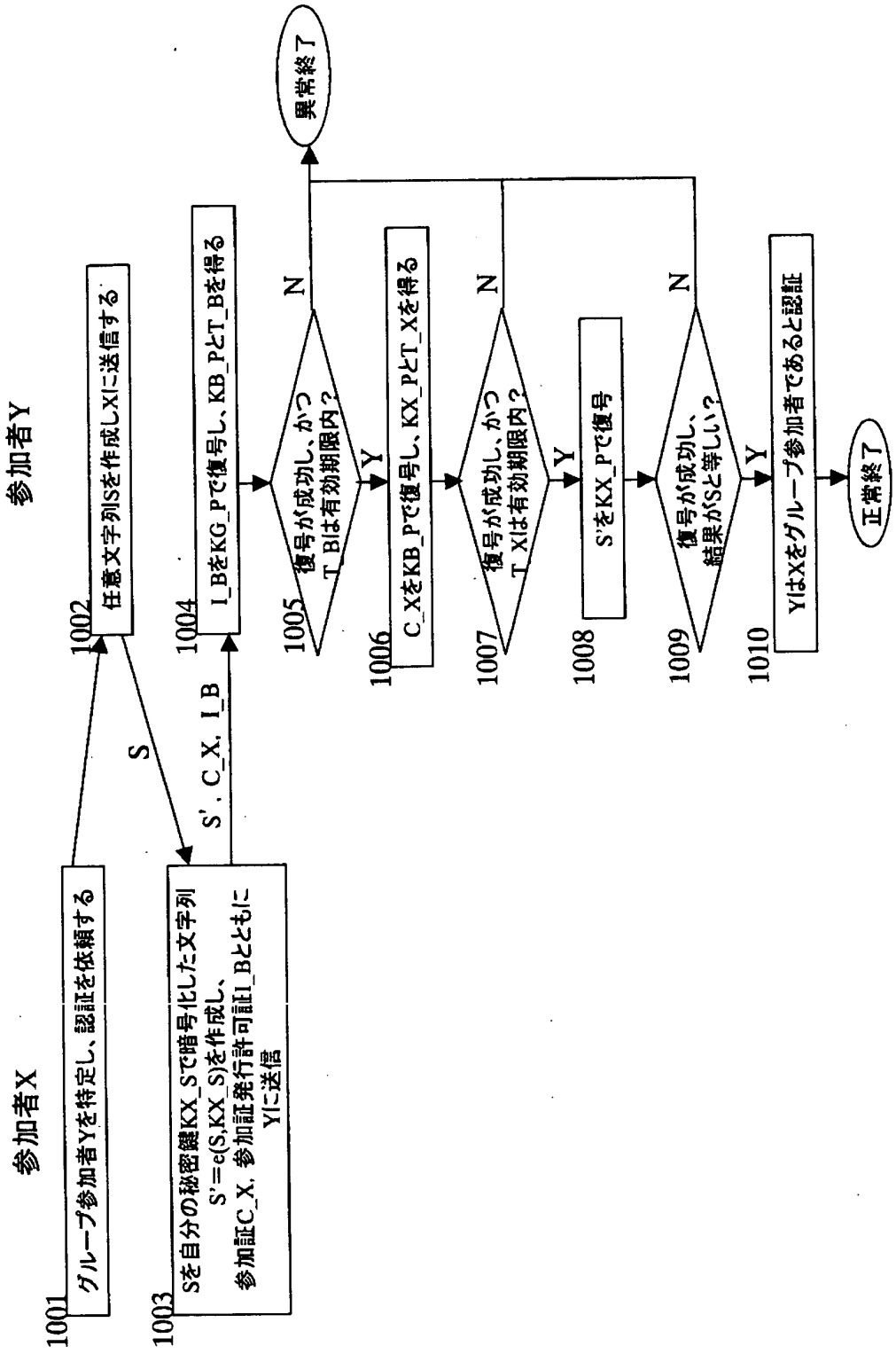
【図８】

KX_P:Xの公開鍵
KX_S:Xの秘密鍵
KG_P:グループの公開鍵
I_B=e(KB_P+T_B,KG_S)
　:Bのグループ参加証発行許可証
C_X=e(KX_P+T_X,KB_S):Xのグループ参加証

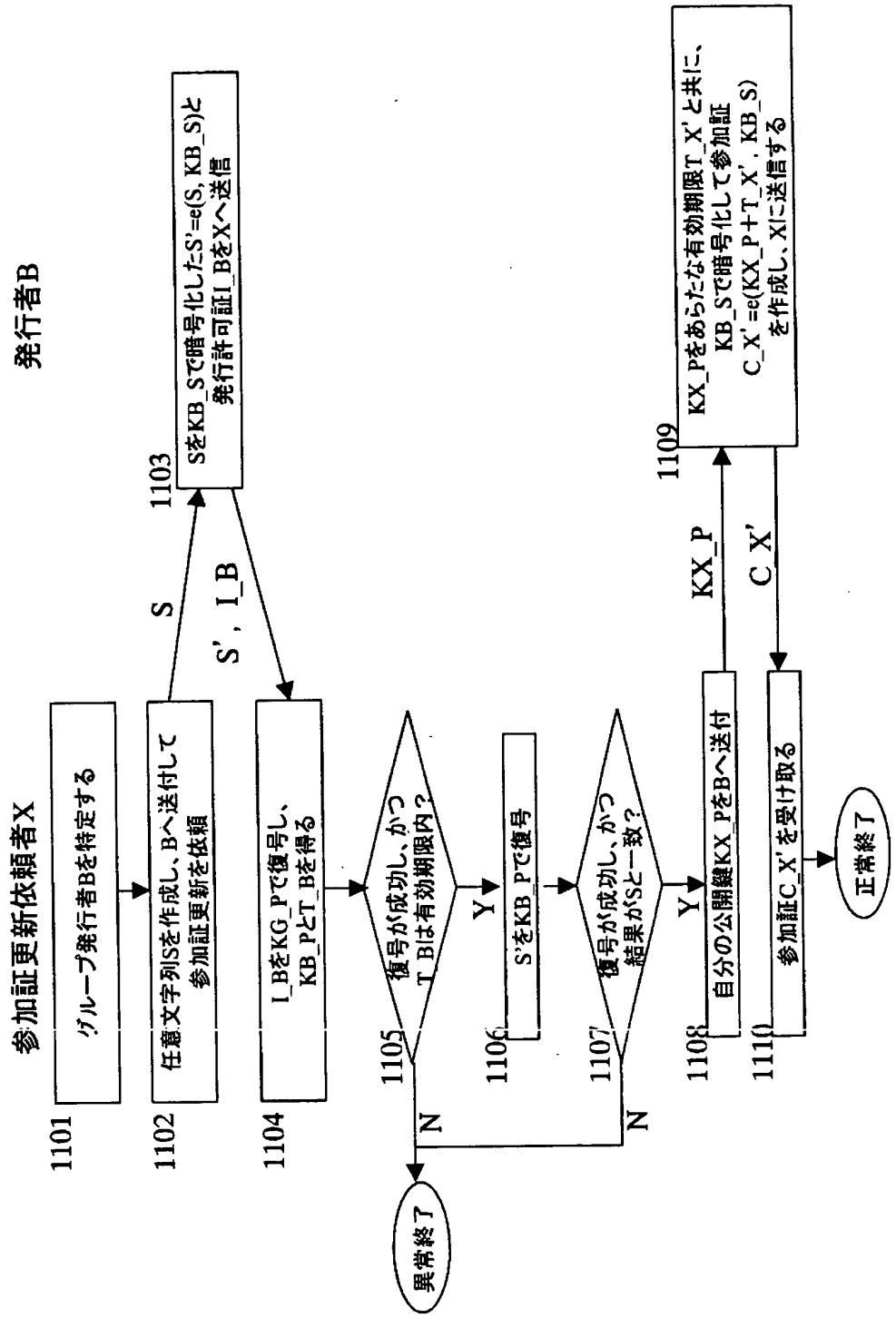
【図９】

KY_P:Yの公開鍵
KY_S:Yの秘密鍵
KG_P:グループの公開鍵
I_C=e(KC_P+T_C,KG_S)
　:別の発行者Cのグループ参加証発行許可証
C_Y=e(KX_P+T_X,KB_S)
　:Cが発行したYのグループ参加証

【図１０】


参加者X
参加者Y
1001
グループ参加者Yを特定し、認証を依頼する
1002
任意文字列Sを作成しXに送信する
S
1003
Sを自分の秘密鍵KX_Sで暗号化した文字列
S'=e(S,KX_S)を作成し、
参加証C_X, 参加証発行許可証I_Bとともに
Yに送信
S', C_X, I_B
1004
I_BをKG_Pで復号し、KB_PとT_Bを得る
1005
復号が成功し、かつ
T_Bは有効期限内？
N
異常終了
Y
1006
C_XをKB_Pで復号し、KX_PとT_Xを得る
1007
復号が成功し、かつ
T_Xは有効期限内？
N
Y
1008
S'をKX_Pで復号
1009
復号が成功し、
結果がSと等しい？
N
Y
1010
YはXをグループ参加者であると認証
正常終了

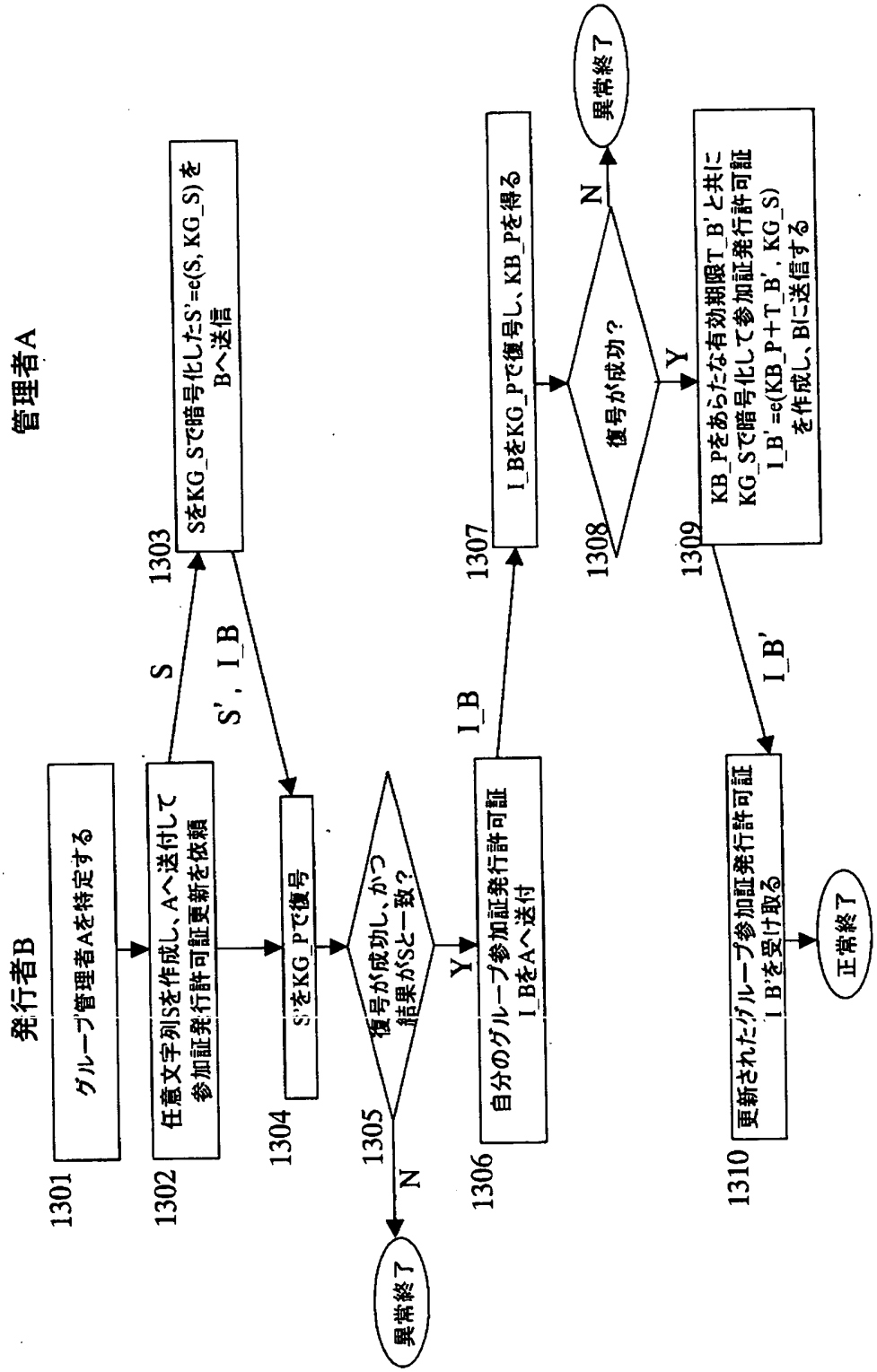
【図１１】


参加証更新依頼者X
発行者B
1101
グループ発行者Bを特定する
1102
任意文字列Sを作成し、Bへ送付して
参加証更新を依頼
S
1103
SをKB_Sで暗号化したS'=e(S, KB_S)と
発行許可証I_BをXへ送信
S', I_B
1104
I_BをKG_Pで復号し、
KB_PとT_Bを得る
1105
復号が成功し、かつ
T_Bは有効期限内？
Y
N
異常終了
1106
S'をKB_Pで復号
1107
復号が成功し、かつ
結果がSと一致？
Y
N
1108
自分の公開鍵KX_PをBへ送付
KX_P
1109
KX_Pをあらたな有効期限T_X'と共に、
KB_Sで暗号化して参加証
C_X'=e(KX_P+T_X', KB_S)
を作成し、Xに送信する
C_X'
1110
参加証C_X'を受け取る
正常終了

【図１２】

KX_P:Xの公開鍵
KX_S:Xの秘密鍵
KG_P:グループの公開鍵
I_B=e(KB_P+T_B,KG_S)
　:Bのグループ参加証発行許可証
C_X=e(KX_P+T_X',KB_S):Xのグループ参加証

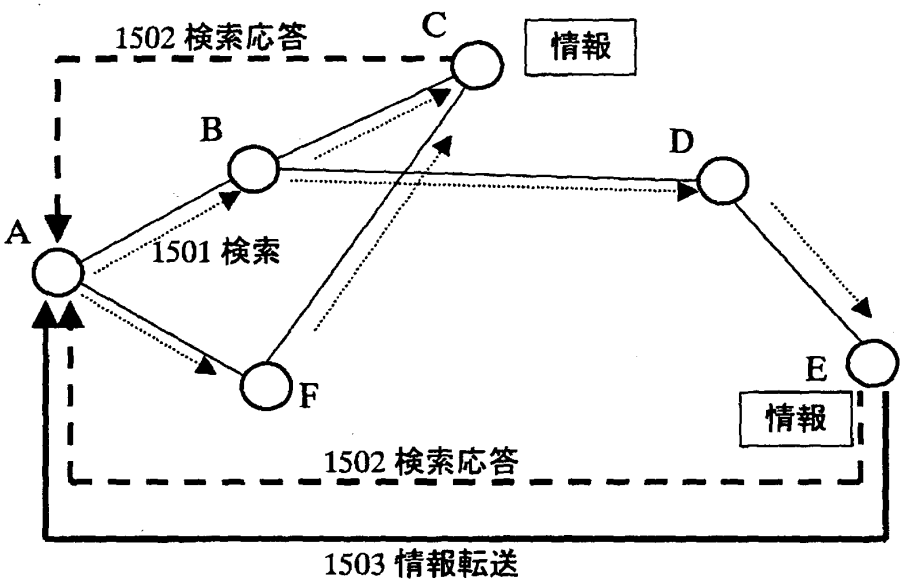
【図１３】


発行者B
管理者A
グループ管理者Aを特定する
1301
任意文字列Sを作成し、Aへ送付して参加証発行許可証更新を依頼
1302
S
S', I_B
SをKG_Sで暗号化したS'=e(S, KG_S)をBへ送信
1303
S'をKG_Pで復号
1304
復号が成功し、かつ結果がSと一致?
1305
N
異常終了
Y
自分のグループ参加証発行許可証I_BをAへ送付
1306
I_B
I_BをKG_Pで復号し、KB_Pを得る
1307
復号が成功?
1308
N
異常終了
Y
KB_Pをあらたな有効期限T_B'と共にKG_Sで暗号化して参加証発行許可証I_B'=e(KB_P+T_B', KG_S)を作成し、Bに送信する
1309
I_B'
更新されたグループ参加証発行許可証I_B'を受け取る
1310
正常終了

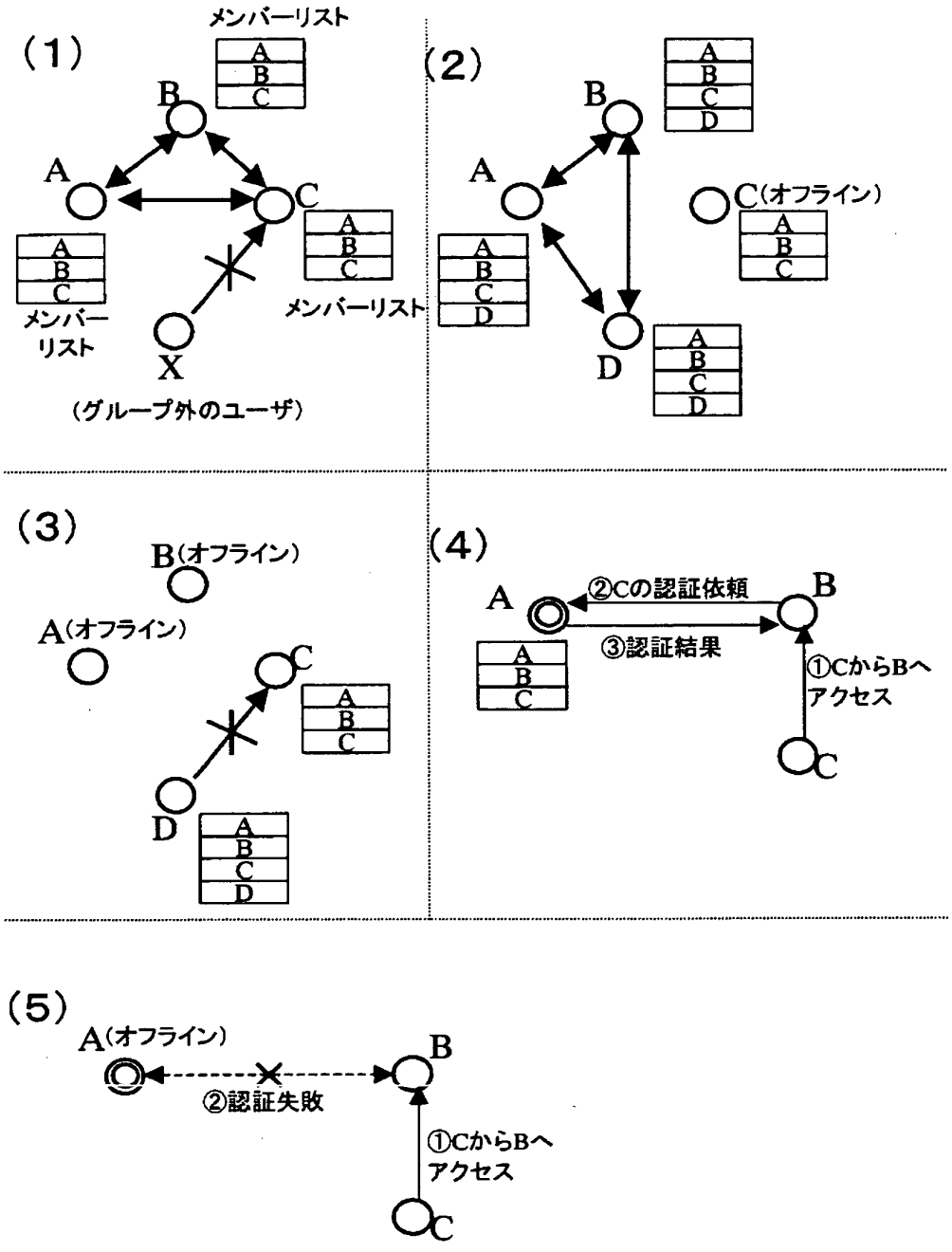
【図１４】

KB_P:Bの公開鍵
KB_S:Bの秘密鍵
KG_P:グループの公開鍵
I_B'=e(KB_P+T_B',KG_S)
:Bのグループ参加証発行許可証

【図１５】



【図１６】


(1)
メンバーリスト
A
B
C
A
B
C
メンバーリスト
A
B
C
メンバーリスト
X
(グループ外のユーザ)
(2)
A
B
C
D
A
B
C
D
C(オフライン)
A
B
C
D
A
B
C
D
(3)
B(オフライン)
A(オフライン)
C
A
B
C
D
A
B
C
D
(4)
A
②Cの認証依頼
B
③認証結果
A
B
C
①CからBへ
アクセス
C
(5)
A(オフライン)
B
②認証失敗
①CからBへ
アクセス
C

【書類名】　要約書

【要約】

【課題】　常時稼動するサーバの運用が不要であり、常に任意のメンバ間で互いに認証が可能。

【解決手段】　管理者あるいは発行者が発行する参加証に基づいてグループメンバ間で互いにグループに属することを認証する。

【選択図】　図１

出証特２００３－３０４５９８７

出 願 人 履 歴 情 報

識別番号　〔０００００５８２１〕

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社